MS221 Chapter D2

The Open University

A second level interdisciplinary course

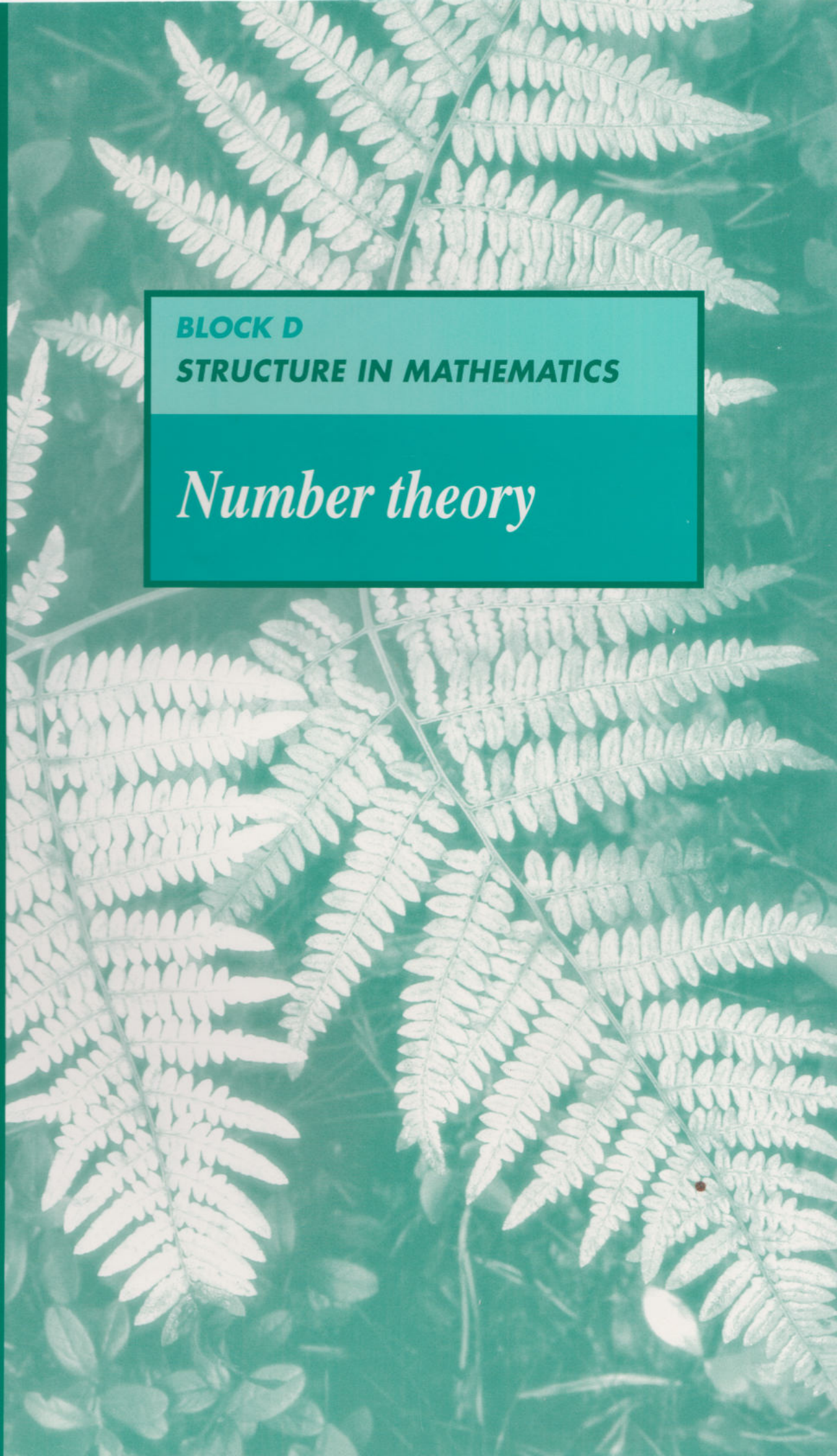
Exploring Mathematics

BLOCK D

STRUCTURE IN MATHEMATICS

Number theory

CHAPTER D2



MS221 Chapter D2

The Open University

A second level interdisciplinary course

Exploring Mathematics

CHAPTER D2

BLOCK D

STRUCTURE IN MATHEMATICS

Number theory

Prepared by the course team

About this course

This course, MS221 *Exploring Mathematics*, and the courses MU120 *Open Mathematics* and MST121 *Using Mathematics* provide a flexible means of entry to university-level mathematics. Further details may be obtained from the address below.

MS221 uses the software program Mathcad (MathSoft, Inc.) to investigate mathematical concepts and as a tool in problem solving. This software is provided as part of the course.

This publication forms part of an Open University course. Details of this and other Open University courses can be obtained from the Course Information and Advice Centre, PO Box 724, The Open University, Milton Keynes, MK7 6ZS, United Kingdom: tel. +44 (0)1908 653231, e-mail general-enquiries@open.ac.uk

Alternatively, you may visit the Open University website at http://www.open.ac.uk where you can learn more about the wide range of courses and packs offered at all levels by The Open University.

To purchase a selection of Open University course materials, visit the webshop at www.ouw.co.uk, or contact Open University Worldwide, Michael Young Building, Walton Hall, Milton Keynes, MK7 6AA, United Kingdom, for a brochure: tel. +44 (0)1908 858785, fax +44 (0)1908 858787, e-mail ouwenq@open.ac.uk

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 1997. Second edition 2004.

Edited, designed and typeset by The Open University, using the Open University TEX System.

Printed and bound in the United Kingdom by The Charlesworth Group, Huddersfield.

ISBN 0 7492 6653 8

2.1

Contents

Study guide

This chapter is best studied in the following four sessions.

Study session 1: Sections 1 and 2.
Study session 2: Section 3.
Study session 3: Section 4.
Study session 4: Section 5.

The first two sessions are longer than the other two, the last of which is based on Mathcad. Subsection 3.4 will not be assessed.

If you prefer a short first session, then note that Section 2 may be studied at any time after Section 1. Also note that, although the Mathcad activities have been presented at the end of the chapter, there are margin notes throughout the earlier sections suggesting other appropriate points at which to try them.

Throughout this chapter there is a lot of arithmetic for you to do and for you to check (if you wish to). So make sure that your calculator is to hand whenever you work on the chapter. Of course, you may prefer to do arithmetic with the aid of Mathcad (when this is convenient).

This chapter contains a number of formally stated results and their proofs. It is not intended that you should be able to construct such proofs for yourself, but you should aim to work through as many as you can. Make a serious effort to understand each proof, but do so within a timetable which ensures that you complete your study of the chapter in a reasonable time.

The optional Video Band D(iii), *Algebra workout — Modular arithmetic*, could be viewed at any stage during your study of this chapter.

Introduction

In this chapter we return to basics and look more closely at the positive integers $1, 2, 3, \ldots$, and their properties. The careful study of these numbers goes back at least to the Ancient Babylonians who knew, for example, how to find triples of positive integers x, y and z, such that

$$x^2 + y^2 = z^2.$$

For example,

$$3^2 + 4^2 = 5^2$$

and

$$5^2 + 12^2 = 13^2.$$

But it was the Ancient Greeks who made the first serious development of what is now called number theory. For example, Euclid studied the prime numbers

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots,$$

It is conventional *not* to include 1 as a prime number.

those positive integers which cannot be expressed as a product of smaller factors and showed, by an ingenious argument, that there are infinitely many such numbers. On the other hand, Euclid seems to have taken for granted that every positive integer greater than 1 has a unique prime factorisation; that is, it can be expressed as a product of prime numbers in only one way (apart from the order of the prime numbers). Though true, this fact is not at all obvious!

After the Ancient Greeks, there was little work done on number theory in the western world until the 17th Century when the French amateur mathematician P. de Fermat took up the subject and discovered many results which now form its foundations. Unfortunately, Fermat published few proofs and it was left to his successors, L. Euler and C. F. Gauss, to establish these foundations securely, and develop the subject further. However, Fermat's influence continues to be felt, partly because he left later generations of mathematicians one of their most challenging problems:

For example, Gauss was the first to publish a proof of the above result on unique prime factorisation.

> Do there exist positive integers x, y, z and n, with $n \geq 3$, such that
>
> $$x^n + y^n = z^n?$$

This was finally answered in 1994, after many earlier attempts.

See Subsection 3.4.

Number theory abounds with tantalising problems of this type, which are studied for their own intrinsic interest, with no view to applications. This does not mean that the subject is without applications, though the English mathematician G. H. Hardy clearly felt that there were none when he wrote:

> If the theory of numbers could be employed for any practical and obviously honourable purpose, if it could be turned directly to the furtherance of human happiness or the relief of human suffering, as physiology and even chemistry can, then surely neither Gauss nor any other mathematician would be so foolish as to decry or regret such applications. But science works for evil as well as for good (and particularly, of course, in time of war); and both Gauss and lesser mathematicians may be justified in rejoicing that there is one science at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.

From Hardy, G. H. (1940) *A Mathematician's Apology*, Cambridge, Cambridge University Press.

In this chapter you will meet some of the basic techniques used in number theory. In particular you will encounter a theorem of Fermat's about prime numbers which Hardy would have regarded as elegant but essentially

trivial, and you will see that this 'trivial' theorem has turned out to have fundamental applications in the very practical area of cryptography!

In order to feel confident about the truth of such theorems and their applications, it is essential that clear reasoning is used to justify them. You will find that this chapter includes a larger number of results and their proofs than earlier ones, and this makes it somewhat more abstract.

The results in the chapter have been labelled with the usual names found in mathematics texts:

- ◇ a **theorem** is a key result, or list of key results;
- ◇ a **lemma** is a minor result, usually preparing the way for a theorem;
- ◇ a **corollary** is a straightforward consequence of a theorem, often a special case of it.

Strictly speaking, there is no formal difference between these types of results — they could all be called theorems. The names have been chosen to give some indication of the relationship between, and relative importance of, the results. They might have been chosen differently by a different author.

Finally, note that in this chapter we shall not discuss the general topic of 'methods of proof'. This will be tackled in Chapter D4.

1 Congruence

1.1 Division

At an early age we learn how to divide one positive integer by another to obtain a quotient and a remainder. For example, 32 divided by 5 gives quotient 6 and remainder 2, because $32 = 6 \times 5 + 2$. In general, if we divide any positive integer by 5, then the remainder will be one of the numbers 0, 1, 2, 3, 4.

Occasionally, we shall need to divide a negative integer by a positive integer. You might guess that, since $-32 = -6 \times 5 - 2$, the quotient would be -6 and the remainder -2. However, when studying the properties of integers it is more convenient to insist that the remainder on division by 5 is always one of the numbers 0, 1, 2, 3, 4. With this preference in mind, we can write

$$-32 = -7 \times 5 + 3$$

to give the quotient -7 and remainder 3.

Experience with long division suggests that a division process of this type can be carried out for any given integer a and positive integer n. Since this is so important in what follows, we state it as our first theorem.

Theorem 1.1 Division Algorithm
Let a and n be integers, with n positive. Then there are unique integers q and r such that

$$a = qn + r, \quad \text{with} \quad 0 \leq r < n.$$

Strictly speaking, this theorem is not an algorithm, but 'Division Algorithm' is the traditional name for it.

The number q is called the **quotient** and r is called the **remainder**, on division by n. If $r = 0$, then we say that a is **divisible** by n, and in this case n is called a **divisor** or **factor** of a.

To see why this theorem is true, we mark the (integer) multiples of n on a number line and then observe in which of the resulting intervals of length n the integer a lies. Let a lie in the interval from qn to $(q+1)n$, as in Figure 1.1.

In this chapter a *multiple* is always an integer multiple.

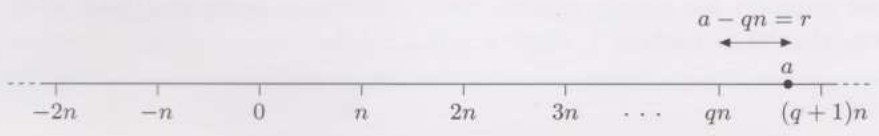


Figure 1.1

This picture should convince you that there is a unique integer q such that

$$qn \leq a < (q+1)n. \tag{1.1}$$

Thus, if we put $r = a - qn$, then $a = qn + r$ and $0 \leq r < n$. This is the required result.

Theorem 1.1 describes what we shall mean by division of an integer a by a positive integer n. If a happens to be positive, then the quotient q and

remainder r can be found by long division. When working with a calculator, however, it is convenient to rewrite (1.1) in the form

$$q \leq \frac{a}{n} < q+1, \quad \text{which implies that} \quad q = \text{floor}\left(\frac{a}{n}\right).$$

Here floor(x) is the greatest integer which is less than or equal to x. In most mathematics texts, this function is denoted by $[x]$.

For example, if $a = 1000$ and $n = 13$, then

$$q = \text{floor}\left(\frac{1000}{13}\right) = \text{floor}(76.92\ldots) = 76,$$

so

We have $r = a - qn$.

$$r = 1000 - 76 \times 13 = 1000 - 988 = 12.$$

This method also works if a is negative. For example, if $a = -1000$ and $n = 13$, then

$$q = \text{floor}\left(\frac{-1000}{13}\right) = \text{floor}(-76.92\ldots) = -77,$$

so

$$r = -1000 - (-77) \times 13 = -1000 + 1001 = 1.$$

Activity 1.1 Practising division

For each of the following integers a and n, find the quotient and remainder on division of a by n.

(a) $a = 77$, $n = 9$

(b) $a = -100$, $n = 11$

(c) $a = 987\,654\,321$, $n = 8$

Solutions are given on page 42.

Activity 1.2 Sharing remainders

Draw a number line and mark on it all the integers between -9 and 9 which give remainder 1 on division by 3. What pattern do you notice?

Comment

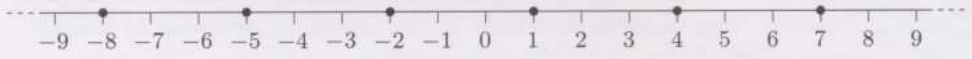


Figure 1.2

These numbers are evenly spaced, their differences being multiples of 3. Notice that they include 1, since $1 = 0 \times 3 + 1$.

1.2 Congruences and their properties

Suppose that n is a positive integer. The outcome of Activity 1.2 suggests that the following assertions about two integers a and b are closely related:

(1) a and b have the same remainder on division by n;
(2) a and b differ by a multiple of n.

In fact these assertions are *equivalent* to each other, in the sense that if (1) is true then (2) is true and, conversely, if (2) is true then (1) is true.

For example, suppose that (1) is true. Then, by the Division Algorithm,

$$a = pn + r \quad \text{and} \quad b = qn + r,$$

where p and q are quotients and r is the common remainder. Thus

$$a - b = (pn + r) - (qn + r) = (p - q)n,$$

so a and b do indeed differ by a multiple of n; that is, (2) is true. We now ask you to try and prove the *converse* result that if (2) is true then (1) is true.

Activity 1.3 A proof

Prove that if (2) is true, then (1) is true.

(One approach is to assume that a has remainder r on division by n, and use the fact that $a - b$ is a multiple of n to deduce that b also has remainder r on division by n.)

A solution is given on page 42.

Since integers with the same remainder on division by n are so closely related in this way, it is useful to introduce the following terminology and notation. This was invented by the great German mathematician C. F. Gauss and appeared in his book *Disquisitiones Arithmeticae* (1801), where he laid the foundations of modern number theory.

Definition

Let n be a positive integer. Two integers a and b are **congruent modulo** n if $a - b$ is a multiple of n; that is, if a and b have the same remainder on division by n.

In symbols we write

$$a \equiv b \pmod{n}.$$

Such a statement is called a **congruence**, and n is called the **modulus** of the congruence.

We say 'a is congruent to b modulo n'.

You have seen other meanings for the word 'modulus' in this course. It is important to interpret technical terms according to the current context.

The word congruent means 'the same'; two numbers which are congruent modulo n are the same, apart from multiples of n.

For example,

$$3 \equiv 25 \pmod{11}, \text{ since } 3 - 25 = -22 \text{ is a multiple of } 11,$$

and

$$7 \equiv -26 \pmod{11}, \text{ since } 7 - (-26) = 33 \text{ is a multiple of } 11.$$

It is usually convenient to check a congruence by considering the difference $a - b$.

On the other hand, 12 and 8 are not congruent modulo 11, since $12 - 8 = 4$ is not a multiple of 11. In this case, we write $12 \not\equiv 8 \pmod{11}$.

Activity 1.4 Checking congruences

Decide which of the following congruences are true and which are false.

(a) $7 \equiv 3 \pmod 4$ (b) $7 \equiv 3 \pmod 8$ (c) $5 \equiv -3 \pmod 4$

(d) $63 \equiv 63 \pmod{37}$ (e) $35 \equiv -9 \pmod 4$ (f) $-9 \equiv 35 \pmod 4$

Solutions are given on page 42.

Comment

Notice that changing the modulus of a congruence, as in parts (a) and (b), may affect the truth of the congruence.

The examples in Activity 1.4 may have suggested to you that congruences have various general properties, and can even be combined in certain ways. For example, the congruences

$$7 \equiv 3 \pmod 4, \quad 5 \equiv -3 \pmod 4, \quad 35 \equiv -9 \pmod 4,$$

suggest that two given congruences can be 'multiplied' to produce a new congruence. Our next theorem gives a list of such basic properties of congruences.

Theorem 1.2 Properties of Congruences

Let n and k be positive integers, and a, b, c, d be integers. Then

(a) $a \equiv a \pmod n$;

(b) if $a \equiv b \pmod n$, then $b \equiv a \pmod n$;

(c) if $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$;

(d) if $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a + c \equiv b + d \pmod n$;

(e) if $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$;

(f) if $a \equiv b \pmod n$, then $a^k \equiv b^k \pmod n$.

This list may look rather forbidding, but each of these six properties is quite simple.

Properties (a), (b) and (c) are easy to prove; for example, the truth of property (c) is evident if it is rewritten as follows: if a and b have the same remainder on division by n, and b and c also have the same remainder on division by n, then this is also true of a and c. This property enables us to string together a list of congruences with the modulus at the end:

$$a \equiv b \equiv c \pmod n.$$

To prove property (d), note that if $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then

$$a - b = kn \quad \text{and} \quad c - d = ln, \tag{1.2}$$

for some integers k and l. Adding these two equations gives

$$(a - b) + (c - d) = kn + ln;$$

that is,

$$(a + c) - (b + d) = (k + l)n,$$

which implies that $a + c \equiv b + d \pmod n$, since $k + l$ is an integer.

Activity 1.5 Subtracting congruences

Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a - c \equiv b - d \pmod{n}.$$

A solution is given on page 42.

The proof of property (e) also follows from equations (1.2), by writing

$$\begin{aligned} ac &= (b + kn)(d + ln) \\ &= bd + n(kd + lb + kln). \end{aligned}$$

Since $kd + lb + kln$ is an integer, this shows that $ac - bd$ is a multiple of n, and hence that $ac \equiv bd \pmod{n}$.

Finally, property (f) is proved by repeated application of property (e) with $c = a$ and $d = b$. Since $a \equiv b \pmod{n}$, we deduce that

$$a^2 \equiv b^2 \pmod{n} \text{ and hence } a^3 \equiv b^3 \pmod{n},$$

and so on. Thus if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$, for all positive integers k.

Here we use

$$a^2 = a \times a$$
$$a^3 = a \times a^2$$

and so on.

It is property (f) which shows how powerful this idea of congruence can be. For example, consider the congruence

$$71 \equiv -1 \pmod{8}.$$

There is nothing remarkable about this congruence, but let us now apply property (f) to it, with $k = 1000$. We deduce that

$$71^{1000} \equiv (-1)^{1000} \pmod{8}; \quad \text{that is,} \quad 71^{1000} \equiv 1 \pmod{8},$$

because 1000 is an *even* integer. Thus 71^{1000} has remainder 1 on division by 8.

The number 71^{1000} is huge. It would be extremely difficult to determine its value and then discover its remainder on division by 8 directly. With property (f), however, we obtain the answer immediately. Moreover, we know that the remainder on division by 8 would still be 1 if we replaced 1000 by 10 000, or indeed by any even positive integer!

Certainly this number is too large for your calculator to handle.

Before offering you the chance to try your hand at finding remainders of these 'high-powered' numbers, we give a slightly more complicated example. In this example, we want to find the remainder when 3^{1000} is divided by 13. The approach we use is to calculate the remainders on division by 13 of the successive powers of 3, continuing until a repeating pattern emerges.

We deal with the first few powers directly:

$$3^1 \equiv 3 \pmod{13}, \; 3^2 \equiv 9 \pmod{13}, \; 3^3 \equiv 27 \equiv 1 \pmod{13}.$$

Although $3^1 = 3$, $3^2 = 9$ and $3^3 = 27$, it looks neater to use $\equiv$ when working with congruences.

Now, we repeatedly multiply by 3 and use property (e):

$$3^4 \equiv 3 \pmod{13}, \; 3^5 \equiv 9 \pmod{13}, \; 3^6 \equiv 1 \pmod{13}.$$

Thus, the remainders form the repeating sequence $3, 9, 1, 3, 9, 1, \ldots$, with

$$3^k \equiv 1 \pmod{13}, \text{ whenever } k \text{ is a positive multiple of 3.}$$

Since 999 is a multiple of 3,

$$3^{999} \equiv 1 \pmod{13},$$

and so

$$3^{1000} \equiv 3 \pmod{13}.$$

Hence, 3^{1000} has remainder 3 on division by 13.

Activity 1.6 Finding remainders by repeated multiplication

You can check your answers to this activity by using the Mathcad file 221D2-01.

Use repeated multiplication to find the remainder when

(a) 2^{38} is divided by 7;

(b) 4^{100} is divided by 10;

(c) 5^{100} is divided by 7.

Comment

(a) $2^1 \equiv 2 \pmod{7}$, $2^2 \equiv 4 \pmod{7}$, $2^3 \equiv 8 \equiv 1 \pmod{7}$, so

$$2^k \equiv 1 \pmod{7}, \text{ whenever } k \text{ is a positive multiple of 3.}$$

Hence $2^{36} \equiv 1 \pmod{7}$ and so

$$2^{38} \equiv 2^{36} \times 2^2 \equiv 1 \times 4 \equiv 4 \pmod{7}.$$

Thus the remainder is 4.

(b) $4^1 \equiv 4 \pmod{10}$, $4^2 \equiv 16 \equiv 6 \pmod{10}$, $4^3 \equiv 24 \equiv 4 \pmod{10}$, so

$$4^k \equiv 4 \pmod{10}, \text{ whenever } k \text{ is an odd positive integer.}$$

Hence $4^{99} \equiv 4 \pmod{10}$ and so

$$4^{100} \equiv 6 \pmod{10}.$$

Thus the remainder is 6.

(c) $5^1 \equiv 5 \pmod{7}$, $5^2 \equiv 25 \equiv 4 \pmod{7}$, $5^3 \equiv 20 \equiv 6 \pmod{7}$, $5^4 \equiv 30 \equiv 2 \pmod{7}$, $5^5 \equiv 10 \equiv 3 \pmod{7}$, $5^6 \equiv 15 \equiv 1 \pmod{7}$, so

$$5^k \equiv 1 \pmod{7}, \text{ whenever } k \text{ is a positive multiple of 6.}$$

Hence $5^{96} \equiv 1 \pmod{7}$ and so

$$5^{100} \equiv 5^{96} \times 5^4 \equiv 1 \times 2 \equiv 2 \pmod{7}.$$

Thus the remainder is 2.

In Activity 1.6(c) you may have begun to wonder whether the process of taking higher and higher powers will *always* lead to a repeating pattern of remainders. The answer to this question is 'yes'. The remainders all belong to the same set of integers $0, 1, 2, \ldots, n-1$, where n is the modulus. So if we carry on calculating powers long enough, then eventually we obtain a remainder that was found earlier, and a repeating pattern must follow. Part (b) shows that remainder 1 does not always appear.

The calculation of these remainders can usefully be arranged in a table of the following kind.

See Activity 1.6(c).

5^k	5^0	5^1	5^2	5^3	5^4	5^5	5^6	5^7	...	5^{96}	...	5^{100}
$5^k \pmod{7}$	1	5	4	6	2	3	1	5	...	1	...	2

It helps to spot repeating patterns by including the entries for $k = 0$.

Warning

We have made repeated use in these calculations of the fact that congruences can be 'multiplied' by an integer; that is, if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$.

This is a special case of Theorem 1.2, property (e). However, congruences cannot, in general, be 'divided' by an integer; a counter-example is

$$10 \equiv 6 \pmod{4} \quad \text{but} \quad 5 \not\equiv 3 \pmod{4}.$$

A *counter-example* is an example which shows that an assertion is false.

1.3 Repeated squaring

In some applications, we need to find remainders when much larger numbers are involved. For example, even to find the remainder of 14^{27} on division by 55, involves calculating the following remainders.

See Section 4.

14^k	14^0	14^1	14^2	14^3	...	14^7	...	14^{10}	...	14^{20}	...	14^{27}
$14^k \pmod{55}$	1	14	31	49	...	9	...	1	...	1	...	9

This calculation is evidently tedious, involving repeated multiplication by 14 and then finding of remainders modulo 55.

A more efficient method, especially for large numbers, uses the idea of *repeated squaring*. This enables us to calculate the remainders on division by 55 of $14^1, 14^2, 14^4, 14^8, \ldots$.

$$14^1 \equiv 14 \pmod{55}$$
$$14^2 \equiv 196 \equiv 31 \pmod{55}$$
$$14^4 \equiv (14^2)^2 \equiv 31^2 \equiv 961 \equiv 26 \pmod{55}$$
$$14^8 \equiv (14^4)^2 \equiv 26^2 \equiv 676 \equiv 16 \pmod{55}$$
$$14^{16} \equiv (14^8)^2 \equiv 16^2 \equiv 256 \equiv 36 \pmod{55}$$

Now, we can express 27 as the sum of powers of 2 as follows:

$$27 = 1 + 2 + 8 + 16.$$

Thus

$$\begin{aligned} 14^{27} &\equiv 14^1 \times 14^2 \times 14^8 \times 14^{16} \pmod{55} \\ &\equiv 14 \times 31 \times 16 \times 36 \pmod{55} \\ &\equiv 249\,984 \equiv 9 \pmod{55}. \end{aligned}$$

Alternatively, use

$$14 \times 31 \equiv 49 \pmod{55},$$
$$49 \times 16 \equiv 14 \pmod{55},$$
$$14 \times 36 \equiv 9 \pmod{55}.$$

A given positive integer k can always be expressed as a sum of powers of 2, as follows. First find the largest power of 2, say 2^m, which is less than or equal to k. Then

$$k = 2^m + k', \text{ where } 0 \leq k' < 2^m.$$

Now repeat this process with k' instead of k, and continue until the remainder term is 0 or 1. For example, $k = 19$ gives

$$19 = 16 + 3,$$

so $k' = 3$ and

$$3 = 2 + 1.$$

Hence

$$19 = 16 + 2 + 1.$$

Activity 1.7 Finding remainders by repeated squaring

You can check your answer to this activity using the Mathcad file 221D2-01.

Use the method of repeated squaring to show that

$$15^{19} \equiv 25 \pmod{55}.$$

A solution is given on page 42.

The calculation of 'repeated squares' remainders can also be arranged in a table.

See the solution to Activity 1.7.

15^{2^n}	15^1	15^2	15^4	15^8	15^{16}	...
$15^{2^n} \pmod{55}$	15	5	25	20	15	...

We shall find such tables useful in Section 4.

Summary of Section 1

In this section you have:

- ◇ met the notion of congruence, which arises by considering remainders on division by positive integers;
- ◇ seen how the rules for manipulating congruences make it possible to determine the remainders of large powers on division by positive integers.

Exercises for Section 1

Exercise 1.1

Use repeated multiplication to find the remainder when

(a) 4^{12} is divided by 11;

(b) 8^{10} is divided by 25.

Exercise 1.2

Find the remainders in Exercise 1.1 using repeated squaring.

2 Divisibility tests

In his book *Further Mathematical Diversions*, Martin Gardner, the celebrated writer of popular mathematics, observed the following.

> A dollar bill that I have just taken from my wallet bears the serial number 61671142. A schoolboy could say at once that this number is exactly divisible by 2 but not by 5. Is it divisible [...] by 3? By 4? By 11? Few people, including many mathematicians, know all the simple rules by which large numbers can be tested quickly for divisibility by numbers 1 through 12. The rules were widely known during the Renaissance, before the invention of decimals, because of their usefulness in reducing large-number fractions to lowest terms. Even today they are handy rules for anyone to know.

In this section, we use congruences to discover simple rules for finding the remainders when a large number, such as 61 671 142, is divided by any positive integer up to and including 13. It may already have occurred to you that such remainders can be found in a few steps using your calculator, but the rules given here can be used for much larger numbers (too large for the calculator to handle directly) should the need arise.

These rules for finding remainders yield simple tests for *divisibility* when used to check for remainder 0.

2.1 Division by 3, 9 and 11

A simple test for divisibility by 3 involves forming the sum of the digits of the given number. If the resulting **digit sum** has more than one digit, then the process is repeated until a single digit remains. The original number is divisible by 3 if and only if this single digit is divisible by 3. For example, with 61 671 142 the successive digit sums are

$$6+1+6+7+1+1+4+2=28, \quad 2+8=10, \quad 1+0=1.$$

Since 1 is not divisible by 3, it follows that 61 671 142 is not divisible by 3.

Let us see why this test works. Consider a positive integer a with digits

$$a_0 \text{ (units)}, \quad a_1 \text{ (tens)}, \quad a_2 \text{ (hundreds)}, \text{ and so on.}$$

Thus

$$a = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots + a_m 10^m,$$

where $m+1$ is the number of digits in a.

For example, $61\,671\,142 = 2 + 4 \times 10 + 1 \times 10^2 + \cdots + 6 \times 10^7$.

Now we use the fact that $10 \equiv 1 \pmod 3$ to deduce, by Theorem 1.2, property (f), that

$$10^1 \equiv 1 \pmod 3, \quad 10^2 \equiv 1 \pmod 3, \quad 10^3 \equiv 1 \pmod 3, \ldots . \tag{2.1}$$

Next we use Theorem 1.2, properties (d) and (e), to deduce that

$$\begin{aligned} a &\equiv a_0 + a_1 \times 1 + a_2 \times 1 + \cdots + a_m \times 1 \pmod 3 \\ &\equiv a_0 + a_1 + a_2 + \cdots + a_m \pmod 3. \end{aligned}$$

Therefore, a and its digit sum have the same remainder on division by 3, as do all the successive digit sums.

For example, the numbers

$$61\,671\,142, \quad 28, \quad 10, \quad 1$$

all have remainder 1 on division by 3.

Activity 2.1 Division by 3

Find the remainder when

6341 7231 1083 2864 is divided by 3.

This 16 digit number is presented as you might see it on a credit card.

Comment

The successive digit sums are 59, 14, 5, and so the remainder on division by 3 is 2.

You could have deduced the answer directly from the first digit sum, 59.

Activity 2.2 Division by 9

(a) Explain why the digit sum method described above also works for division by 9.

(b) Find the remainder when

6341 7231 1083 2864 is divided by 9.

Comment

(a) The digit sum method depends on congruences (2.1) and these congruences also hold modulo 9, because $10 \equiv 1 \pmod 9$. Therefore the digit sum method works for division by 9.

(b) Using the digit sums found in Activity 2.1, we find that the remainder on division by 9 is 5.

The divisibility test for 11 is slightly different. It uses the fact that $10 \equiv -1 \pmod{11}$, from which we deduce that

$$10^k \equiv (-1)^k \pmod{11}, \quad \text{for } k = 1, 2, \ldots .$$

Here

$10^2 \equiv 1 \pmod{11}$,
$10^3 \equiv -1 \pmod{11}$,
$10^4 \equiv 1 \pmod{11}$,

and so on.

Therefore, if

$$a = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots + a_m \times 10^m,$$

then

$$a \equiv a_0 - a_1 + a_2 - \cdots + (-1)^m a_m \pmod{11}.$$

Thus a has the same remainder on division by 11 as its **alternating digit sum**, which starts with the *units* digit. For example, with $a = 61\,671\,142$, the alternating digit sum is

$$2 - 4 + 1 - 1 + 7 - 6 + 1 - 6 = 11 - 17 = -6.$$

Since $-6 \equiv 5 \pmod{11}$, it follows that 61 671 142 gives remainder 5 on division by 11.

Activity 2.3 Division by 11

Find the remainder when

6341 7231 1083 2864 is divided by 11.

Comment

The alternating digit sum is

$$4 - 6 + 8 - 2 + 3 - 8 + 0 - 1 + 1 - 3 + 2 - 7 + 1 - 4 + 3 - 6$$
$$= 22 - 37 = -15.$$

Since $-15 \equiv 7 \pmod{11}$, it follows that 6341 7231 1083 2864 gives remainder 7 on division by 11.

Remark

The number being tested may be so large that its alternating digit sum is again quite large. In this case, we can repeat the process of taking the alternating digit sum, as long as we remember to take account of any minus sign which appears. For example, in Activity 2.3 the alternating digit sum of -15 is $-(5-1) = -4$, which is indeed congruent to 7 modulo 11.

2.2 Division by 2, 4, 8, ...

Most people can recognise an even number by looking at its final digit, but rather fewer people can recognise one that is divisible by 4, in spite of the need to identify leap years.

In fact, if

$$a = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots + a_m \times 10^m,$$

then

$$a \equiv a_0 + a_1 \times 10 \pmod{4},$$

since $10^2, 10^3, \ldots$, are all divisible by 4.

Therefore a has the same remainder on division by 4 as the number formed by its final *two* digits. For example, the number formed by the final two digits of 61 671 142 is 42, and so 61 671 142 has remainder 2 on division by 4. Similarly, we can find the remainder on division by $8 = 2^3$, by considering the number formed from the last *three* digits, and so on.

This approach extends to division by 2^k for each positive integer k because 10^k is divisible by 2^k.

Activity 2.4 Division by 4 and 8

Find the remainder when

6341 7231 1083 2864 is divided (a) by 4 and (b) by 8.

Comment

(a) This number is congruent to 64 modulo 4, and so it is divisible by 4; hence the remainder is 0.

(b) This number is congruent to 864 modulo 8, and so it is divisible by 8; hence the remainder is 0.

You may like to check that this number is also divisible by 16 and 32, but not by 64.

2.3 Division by 6 and 12

To test a number for divisibility by 6, we simply apply the tests for divisibility by 2 and by 3, both of which must give the answer 'yes'. The actual remainder, r_6 say, on division by 6 can be deduced from the remainders r_2 and r_3 obtained on division by 2 and by 3. One way to do this is to use the congruence

$$r_6 \equiv 3r_2 - 2r_3 \pmod{6}. \qquad (2.2)$$

We discuss why this congruence holds shortly.

For example, we already know that

$$61\,671\,142 \equiv 0 \pmod 2 \text{ and } 61\,671\,142 \equiv 1 \pmod 3,$$

so $r_2 = 0$, $r_3 = 1$. Hence

$$r_6 \equiv 3r_2 - 2r_3 \equiv -2 \pmod 6,$$

so $r_6 = -2 + 6 = 4$.

A similar approach can be used to calculate the remainder r_{12} on division by 12, given the remainders r_3 and r_4 on division by 3 and 4. In this case we can use the congruence

$$r_{12} \equiv 4r_3 - 3r_4 \pmod{12}. \tag{2.3}$$

For example, since $61\,671\,142 \equiv 1 \pmod 3$ and $61\,671\,142 \equiv 2 \pmod 4$,

$$r_{12} \equiv 4r_3 - 3r_4 \equiv -2 \pmod{12},$$

so $r_{12} = -2 + 12 = 10$.

Activity 2.5 Division by 6 and 12

Find the remainder when

6341 7231 1083 2864 is divided (a) by 6 and (b) by 12.

Solutions are given on page 42.

Activity 2.6 Explanations

Try to explain why the congruences (2.2) and (2.3) are true.

Comment

Suppose that a has remainder r_2 on division by 2 and remainder r_3 on division by 3. This means that

$$a = 2q_2 + r_2 \quad \text{and} \quad a = 3q_3 + r_3,$$

where q_2 and q_3 are the respective quotients. We now manipulate these two equations to obtain a on the left-hand side and multiples of q_2 and q_3 which are divisible by 6 on the right-hand side:

$$\begin{aligned} a &= 3a - 2a \\ &= 3(2q_2 + r_2) - 2(3q_3 + r_3) \\ &= 6q_2 - 6q_3 + 3r_2 - 2r_3. \end{aligned}$$

Thus $a \equiv 3r_2 - 2r_3 \pmod 6$, and so the remainder of a on division by 6 is congruent to $3r_2 - 2r_3$ modulo 6. This justifies congruence (2.2).

A similar reasoning justifies congruence (2.3).

2.4 Division by 7 and 13

There is no very simple rule for divisibility by 7 or by 13 but, for the sake of completeness, we include rules for these. They are at least slightly quicker than long division.

Both rules depend on the intriguing factorisation

$$1001 = 7 \times 11 \times 13,$$

which is the basis of various number tricks. Thus

$$1000 \equiv -1 \pmod 7 \quad \text{and} \quad 1000 \equiv -1 \pmod{13}.$$

We shall consider division by 7 first. If

$$a = a_0 + a_1 \times 10 + a_2 \times 10^2 + a_3 \times 10^3 + a_4 \times 10^4 + a_5 \times 10^5 + \cdots,$$

then

$$a \equiv (a_0 + a_1 \times 10 + a_2 \times 10^2) + 10^3(a_3 + a_4 \times 10 + a_5 \times 10^2) + 10^6(a_6 + a_7 \times 10 + a_8 \times 10^2) + \cdots \pmod 7.$$

Using the fact that $1000 = -1 \pmod 7$, we obtain

$$a \equiv (a_0 + a_1 \times 10 + a_2 \times 10^2) - (a_3 + a_4 \times 10 + a_5 \times 10^2) + (a_6 + a_7 \times 10 + a_8 \times 10^2) + \cdots \pmod 7,$$

which is an alternating sum of 3 digit numbers.

So, if we

- ◇ split a every 3 digits, starting from the right,
- ◇ find the remainder of each 3 digit number on division by 7,
- ◇ form the alternating sum of these remainders,

then the resulting number will be congruent to a modulo 7 (and much smaller than a).

Of course, the *last* number formed by the above splitting may have 1, 2 or 3 digits. For convenience, the phrase '3 digit number' is taken to apply also to the last number even if it has just 1 or 2 digits.

For example, if $a = 61\,671\,142$, then the remainders are as follows.

61	671	142	
5	6	2	(mod 7)

$142 \equiv 2 \pmod 7$
$671 \equiv 6 \pmod 7$
$61 \equiv 5 \pmod 7$

The alternating sum of these remainders is

$$2 - 6 + 5 = 1,$$

and so $a \equiv 1 \pmod 7$. Hence the remainder of a on division by 7 is 1.

Exactly the same rule can be used for division by 13, provided that the remainders are calculated after division by 13. For example, if $a = 61\,671\,142$, then the remainders are

61	671	142	
9	8	12	(mod 13)

and their alternating sum is

$$12 - 8 + 9 = 13.$$

Hence $61\,671\,142 \equiv 13 \pmod{13} \equiv 0 \pmod{13}$, and so 61 671 142 is divisible by 13, as you can readily check on a calculator.

Activity 2.7 Division by 7 and 13

Find the remainder when

6341 7231 1083 2864 is divided (a) by 7 and (b) by 13.

Solutions are given on page 42.

Summary of Section 2

In this section you have seen various simple rules for finding the remainders on division of large numbers by small positive integers.

Exercises for Section 2

Exercise 2.1

State simple rules for finding the remainder when a positive integer is divided by 2, 5 or 10. Explain why these rules hold.

Exercise 2.2

Find the remainders when

5230 6120 0972 1753

is divided by

(a) 2, (b) 3, (c) 4, (d) 5, (e) 6, (f) 7, (g) 8, (h) 9, (i) 10, (j) 11, (k) 12.

Exercise 2.3

(a) A rule for finding the remainder r_{14} when a positive integer a is divided by 14, given the remainders r_2 and r_7 on division of a by 2 and 7, is

$$r_{14} \equiv 7r_2 - 6r_7 \pmod{14}.$$

Explain why this congruence is true.

(b) Use this rule to find the remainder when the integer in Exercise 2.2 is divided by 14.

3 Modular arithmetic

In this section we introduce a new kind of arithmetic, called *modular arithmetic*, and use this arithmetic to derive a remarkable technique for finding the remainder of a large power on division by a prime number.

3.1 Modular addition and multiplication

While reading this subsection you may find it useful to try the Mathcad file 221D2-02.

Let n be a positive integer. Every integer is congruent modulo n to exactly one of the numbers $0, 1, 2, \ldots, n-1$, by the Division Algorithm, and so it is convenient to have a notation for this special set of numbers. The notation $\mathbb{Z}$ for the integers $\{0, \pm 1, \pm 2, \ldots\}$ has been adapted to give

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

For example, $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\}$.

We perform modular arithmetic on $\mathbb{Z}_n$ by using an addition operation $+_n$ and a multiplication operation $\times_n$, which are defined as follows.

Definition

For a and b in $\mathbb{Z}_n$, the **operations $+_n$ and $\times_n$** are defined by:

$a +_n b$ is the remainder on division of $a + b$ by n;

$a \times_n b$ is the remainder on division of $a \times b$ by n.

In words, $a +_n b$ is

'a plus b modulo n'

and $a \times_n b$ is

'a times b modulo n'.

For example, 2 and 4 are both in $\mathbb{Z}_5$ and

$$2 + 4 = 6, \quad \text{so} \quad 2 +_5 4 = 1,$$
$$2 \times 4 = 8, \quad \text{so} \quad 2 \times_5 4 = 3.$$

Modular arithmetic should not be completely new to you, as we regularly use the operation $+_{12}$, for example, when measuring time. For this reason modular arithmetic is sometimes called 'clock arithmetic'.

For example, 2 o'clock is 4 hours after 10 o'clock.

Activity 3.1 Modular arithmetic

Evaluate the following.

(a) $4 +_5 4$, $3 +_6 4$, $1 +_9 3$, $7 +_9 8$, $10 +_{12} 4$

(b) $4 \times_5 4$, $3 \times_6 4$, $1 \times_9 3$, $7 \times_9 8$, $10 \times_{12} 4$

Solutions are given on page 42.

For small values of n, we can conveniently study addition in $\mathbb{Z}_n$ by constructing addition tables, as follows.

$+_2$	0	1
0	0	1
1	1	0

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Activity 3.2 Patterns in the $\mathbb{Z}_n$ addition table

(a) Construct the addition tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

(b) What patterns do you see in these and the earlier addition tables? Try to explain why these patterns occur.

Solutions are given on page 43.

In a similar way, we can construct multiplication tables for $\mathbb{Z}_n$, but here the overall structure of the tables is more mysterious.

$\times_2$	0	1
0	0	0
1	0	1

$\times_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Activity 3.3 Patterns in the $\mathbb{Z}_n$ multiplication table

(a) Construct the multiplication tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

(b) What patterns do you see in these and the earlier multiplication tables? Try to explain why these patterns occur.

(c) Formulate a conjecture about which rows and columns of the multiplication table for $\mathbb{Z}_n$ include *all* the numbers from $\mathbb{Z}_n$.

(*Hint*: In answering this part, consider the factors of n and of the row or column number.)

Solutions are given on page 43.

In the solutions to Activities 3.2 and 3.3, we pointed out that, for all a and b in $\mathbb{Z}_n$,

$$a +_n b = b +_n a \quad \text{and} \quad a \times_n b = b \times_n a.$$

In Chapter D1 you saw that addition and multiplication are commutative and associative on $\mathbb{C}$.

These properties may be described by saying that the operations $+_n$ and $\times_n$ are both *commutative* on the set $\mathbb{Z}_n$. These operations are also *associative* on $\mathbb{Z}_n$; that is, for all a, b and c in $\mathbb{Z}_n$,

$$a +_n (b +_n c) = (a +_n b) +_n c \quad \text{and} \quad a \times_n (b \times_n c) = (a \times_n b) \times_n c.$$

For example,

$$2 \times_5 (3 \times_5 4) = 4$$

and

$$(2 \times_5 3) \times_5 4 = 4.$$

These useful properties enable us to write sums $a +_n b +_n c +_n \cdots$ and products $a \times_n b \times_n c \times_n \cdots$ without the need for brackets.

The proofs of these two associative properties are very similar. We invite you to discover the proof for $+_n$ in the next activity.

Activity 3.4 Proving associativity

Prove that, for all a, b, c in $\mathbb{Z}_n$,

$$a +_n (b +_n c) = (a +_n b) +_n c.$$

(*Hint*: Try to show that both sides of this equation are congruent modulo n to $a + b + c$, using Theorem 1.2.)

A solution is given on page 43.

3.2 Multiplicative inverses

While reading this subsection you may find it useful to try the Mathcad file 221D2-02.

A key question was considered in Activity 3.3:

> Which non-zero rows and columns of the multiplication table for $\mathbb{Z}_n$ include *all* numbers from $\mathbb{Z}_n$?

By inspecting several multiplication tables, we conjectured that the answer to this question has something to do with common factors. We say that two positive integers a and b have a **common factor** c if c is a factor of both a and b; that is, if c is a positive integer which divides exactly into a and b. For example,

> 2 and 4 have common factors 1 and 2,
> 4 and 15 have common factor 1,
> 12 and 18 have common factors 1, 2, 3 and 6.

Clearly, any two positive integers a and b will have $c = 1$ as a common factor. If their only common factor is $c = 1$, then we say that a and b are **coprime** or, equivalently, that a is **coprime with** b. For example, 4 and 15 are coprime, but 12 and 18 are not.

The following discussion is in terms of rows, but it applies equally well to columns.

It appears that row a of the multiplication table for $\mathbb{Z}_n$ includes all numbers in $\mathbb{Z}_n$ if and only if a and n are coprime. We shall prove that this conjecture is true, but first we ask you to practise finding common factors.

Activity 3.5 Finding common factors

(a) Which non-zero numbers in $\mathbb{Z}_9$ are coprime with 9?

(b) Check that only the corresponding rows of the multiplication table for $\mathbb{Z}_9$ include the whole of $\mathbb{Z}_9$.

Solutions are given on page 43.

In all the multiplication tables for $\mathbb{Z}_n$ that we have considered, the appearance of the number 1 in a given row seems to indicate that the row includes *all* numbers in $\mathbb{Z}_n$. We now establish this property.

See pages 22 and 43.

Lemma 3.1
If 1 appears in a row of the multiplication table for $\mathbb{Z}_n$, then each number in $\mathbb{Z}_n$ occurs exactly once in that row.

$\times_n$	0	...	b	...
0	0	...	0	...
⋮	⋮		⋮	
a	0	...	1	...
⋮	⋮		⋮	

Suppose that 1 does appear in row a, say, of the multiplication table for $\mathbb{Z}_n$. This means that there is a number b in $\mathbb{Z}_n$ such that $a \times_n b = 1$.

Now, suppose that c is *any* member of $\mathbb{Z}_n$. Then

$$(a \times_n b) \times_n c = 1 \times_n c = c,$$

so, by the associativity of the operation $\times_n$,

$$a \times_n (b \times_n c) = c.$$

This shows that c lies in column $b \times_n c$ of row a. Hence, since c is any member of $\mathbb{Z}_n$, row a must include the whole of $\mathbb{Z}_n$. Moreover, since $\mathbb{Z}_n$ has n members and row a has n entries, each member of $\mathbb{Z}_n$ occurs exactly once in row a. This proves Lemma 3.1.

Because Lemma 3.1 shows that the number 1 is of such significance in the multiplication table for $\mathbb{Z}_n$, we introduce the following definition.

Definition

Let n, a and b be positive integers with a and b in $\mathbb{Z}_n$, and suppose that $a \times_n b = 1$. Then b is the **multiplicative inverse** of a in $\mathbb{Z}_n$.

We say 'the' multiplicative inverse because, as you will see, there can be at most one.

For example, 8 has multiplicative inverse 5 in $\mathbb{Z}_{13}$ because $8 \times_{13} 5 = 1$, and 5 has multiplicative inverse 2 in $\mathbb{Z}_9$ because $5 \times_9 2 = 1$. On the other hand, 6 has no multiplicative inverse in $\mathbb{Z}_9$ (see row 6 of the table in the solution to Activity 3.5).

We can use Lemma 3.1 to show that if a has a multiplicative inverse, then that multiplicative inverse is unique. If a has a multiplicative inverse, then 1 lies in row a. Hence, by Lemma 3.1, each member of $\mathbb{Z}_n$ appears exactly once in that row. In particular, 1 appears exactly once in row a, and the number at the top of the corresponding column is *the* multiplicative inverse of a.

We now describe a method of finding multiplicative inverses, when they exist. For small values of n, they can be found by trial and error, or by consulting the multiplication table for $\mathbb{Z}_n$ if that is available. However, as n increases in size, the following method becomes much more efficient. It is known as **Euclid's Algorithm**, and was described in Euclid's *Elements*, which dates from around 300 BC.

Suppose, for example, that we wish to find the multiplicative inverse of 9 in $\mathbb{Z}_{25}$; that is, we seek a number b in $\mathbb{Z}_{25}$ such that $9 \times_{25} b = 1$, or, equivalently, such that

$$9b = 25k + 1, \quad \text{for some integer } k. \tag{3.1}$$

We apply the Division Algorithm (Theorem 1.1) repeatedly, first dividing 25 by 9:

$$\begin{aligned} 25 &= 2 \times 9 + 7 \\ 9 &= 1 \times 7 + 2 \\ 7 &= 3 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned} \tag{3.2}$$

At each step we divide the divider in the row above by the remainder in the row above, repeating the process until we reach a remainder of 0 (which must occur, because the remainders decrease by at least one at each step).

We can use the equations (3.2) to find integers b and k which satisfy equation (3.1). To do this, we rearrange the first three of equations (3.2) and put them in reverse order, as follows:

$$1 = 7 - 3 \times 2$$
$$2 = 9 - 1 \times 7$$
$$7 = 25 - 2 \times 9.$$

We now eliminate multiples of 2 and 7 by successive substitutions, as follows:

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - 3(9 - 1 \times 7) \\ &= -3 \times 9 + 4 \times 7 \\ &= -3 \times 9 + 4(25 - 2 \times 9) \\ &= 4 \times 25 - 11 \times 9. \end{aligned}$$

Note that the numbers to be substituted have been kept to the right.

To obtain an equation in the form of (3.1), we rearrange this equation as follows:

$$9 \times (-11) = 25 \times (-4) + 1. \tag{3.3}$$

Thus equation (3.1) holds with $b = -11$ and $k = -4$.

The problem with this solution is that $b = -11$ does not belong to $\mathbb{Z}_{25}$. However, it follows from equation (3.3) that

$$9 \times (-11) \equiv 1 \pmod{25},$$

and since $-11 \equiv 14 \pmod{25}$, we obtain

$$9 \times 14 \equiv 1 \pmod{25}.$$

Hence $b = 14$ is the multiplicative inverse of 9 in $\mathbb{Z}_{25}$.

As a check:

$$\begin{aligned} 9 \times 14 &= 126 \\ &= 5 \times 25 + 1. \end{aligned}$$

Activity 3.6 Finding multiplicative inverses

Use Euclid's Algorithm to find:

(a) the multiplicative inverse of 7 in $\mathbb{Z}_{12}$;

(b) the multiplicative inverse of 9 in $\mathbb{Z}_{26}$.

Solutions are given on page 43.

The above examples indicate that we can find a multiplicative inverse whenever repeated use of the Division Algorithm produces a remainder of 1 at the penultimate step. We now show that the remainder 1 will occur whenever a and n are coprime. Indeed, if we try to use Euclid's Algorithm to find the multiplicative inverse of a in $\mathbb{Z}_n$, then it takes the following form:

$$\begin{aligned} n &= q_1 a + r_1, & 0 < r_1 < a, \\ a &= q_2 r_1 + r_2, & 0 < r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, & 0 < r_3 < r_2, \\ &\vdots \\ r_{m-2} &= q_m r_{m-1} + r_m, & 0 < r_m < r_{m-1}, \\ r_{m-1} &= q_{m+1} r_m + 0, \end{aligned}$$

where m is a positive integer. As noted earlier, the remainders $r_1, r_2, \ldots$, decrease by at least one at each step, so they must eventually reach 0.

The final equation shows that r_m is a factor of r_{m-1}, and then the penultimate equation shows that r_m is also a factor of r_{m-2}. Continuing in this way, we find that r_m is a factor of all the remainders, and so of both a and n. Since a and n were assumed to be coprime, we deduce that $r_m = 1$. Therefore, the penultimate equation has remainder 1, just as we hoped.

If n and a are *not* coprime, then the remainder r_m in Euclid's Algorithm is the *highest common factor* of n and a.

This reasoning shows that if a and n are coprime, then a does have a multiplicative inverse in $\mathbb{Z}_n$. Therefore, we have proved part of the following theorem, which answers the conjecture formulated in Activity 3.3(c).

Theorem 3.1

Let n and a be positive integers, with a in $\mathbb{Z}_n$. The following three statements are equivalent:

(a) a and n are coprime;

(b) a has a multiplicative inverse in $\mathbb{Z}_n$;

(c) row a of the multiplication table for $\mathbb{Z}_n$ includes all of $\mathbb{Z}_n$.

This theorem also holds if 'row' is replaced by 'column'.

To say that these three statements are 'equivalent' means that if any one of the statements is true, then the other two statements are also true.

We have just proved using Euclid's Algorithm that if statement (a) is true, then statement (b) is true. We also know that if statement (b) is true, then statement (c) is true, by Lemma 3.1. Thus to conclude that all three statements are equivalent, we only need to show that if statement (c) is true, then statement (a) is true.

But if row a includes all members of $\mathbb{Z}_n$, then this row certainly includes 1, so a has multiplicative inverse, b say:

$$a \times_n b = 1;$$

that is, $ab \equiv 1 \pmod{n}$, and so

$$ab = kn + 1,$$

for some integer k. But this last equation implies that a and n are coprime, because any common factor of a and n must also be a factor of 1. Thus a and n are coprime, so the proof of Theorem 3.1 is complete.

The following result follows easily from Theorem 3.1.

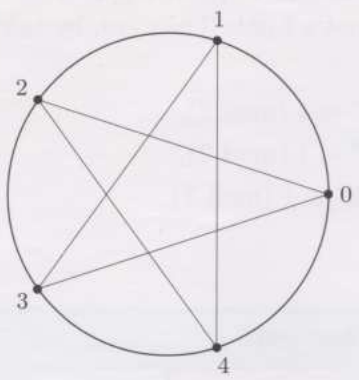
Corollary 3.1

Let p be a prime number. Then each non-zero row of the multiplication table for $\mathbb{Z}_p$ includes the whole of $\mathbb{Z}_p$.

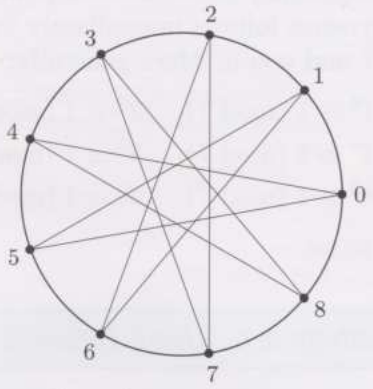
For example, see the multiplication table for $\mathbb{Z}_5$ in the solution to Activity 3.3.

Corollary 3.1 holds because if p is prime, then any positive integer a in $\mathbb{Z}_p$ has no common factor with p which is greater than 1. Indeed, p has no factors other than 1 and p.

This corollary will have a key role to play shortly in a remarkable result about remainders of powers. First, however, we briefly mention the relevance of Theorem 3.1 to **star polygons**. These figures are obtained by placing n points evenly around a circle and joining successive pairs of points which are a points apart on the circle, where $1 < a < n - 1$ (see Figure 3.1). If $a = 1$ or $a = n - 1$, we obtain an ordinary polygon.



$n = 5, a = 2$



$n = 9, a = 5$

Figure 3.1 Two star polygons

If we label the points $0, 1, 2, \ldots, n-1$, as in the diagrams, and call the sequence of points visited on the star polygon $x_0, x_1, \ldots, x_{n-1}$, where $x_0 = 0$, then

$$x_k \equiv ka \pmod{n}, \quad \text{for } k = 0, 1, 2, \ldots, n-1.$$

Therefore, the sequence $x_0, x_1, \ldots, x_{n-1}$ is identical to the sequence of entries in row a of the multiplication table for $\mathbb{Z}_n$. Theorem 3.1 implies that the star polygon passes through all n points on the circle if and only if a and n are coprime, as in the two diagrams above. You may like to experiment to see what happens when a and n are *not* coprime.

If $n = 5$ and $a = 2$, then

$x_0 = 0,$
$x_1 = 2,$
$x_2 = 4,$
$x_3 = 1,$
$x_4 = 3.$

3.3 Fermat's Little Theorem

Pierre de Fermat (1601–1665) was a lawyer in the French city of Toulouse, who became interested in mathematics. Though only an amateur mathematician, he made contributions to number theory that have placed him amongst the 'all-time greats' of the subject.

Fermat did not record his results and proofs systematically, but communicated them by letters to his friends and scribbled them in the margins of his mathematics books. The result we shall now describe was sent by Fermat in 1640 to an acquaintance with the comment 'I'd send you the proof, but I fear that it is too long'. In fact, a proof of the result was first published by Euler 100 years later.

Theorem 3.2 Fermat's Little Theorem
Let p be a prime number, and let a be a positive integer which is not a multiple of p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's Little Theorem is often stated with the conclusion

$$a^p \equiv a \pmod{p},$$

which holds even if a is a multiple of p.

This result certainly counts amongst the gems of mathematics, for it is easy to state, needs very little prior knowledge to understand, is by no means obvious and yet has a short elegant proof (as you will see).

It has an important application to finding remainders of powers modulo p, where p is a prime number. For example, in Activity 1.6(c), you found that

$$5^6 \equiv 1 \pmod{7},$$

by calculating the successive powers of 5 modulo 7. However, this congruence follows immediately from Fermat's Little Theorem, by taking $p = 7$ and $a = 5$. More generally:

$$1^6 \equiv 1 \pmod 7, \quad 2^6 \equiv 1 \pmod 7, \quad 3^6 \equiv 1 \pmod 7,$$
$$4^6 \equiv 1 \pmod 7, \quad 5^6 \equiv 1 \pmod 7, \quad 6^6 \equiv 1 \pmod 7,$$
$$8^6 \equiv 1 \pmod 7, \quad 9^6 \equiv 1 \pmod 7, \quad 10^6 \equiv 1 \pmod 7,$$

and so on.

Of course, $7^6 \equiv 0 \pmod 7$.

Activity 3.7 Using Fermat's Little Theorem

Use Fermat's Little Theorem to find the remainders when

(a) 3^{18} is divided by 19;

(b) 3^{55} is divided by 19;

(c) 16^{103} is divided by 11.

(In part (b), it helps to note that $55 = 3 \times 18 + 1$.)

Solutions are given on page 44.

Remark

Before applying Fermat's Little Theorem, we need to be sure that the number p is prime. We can easily compile a list of the prime numbers up to, say, 100 by inspection:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

The obvious way to check whether a larger number, such as 10 001, is prime is to check it for divisibility by the primes 2, 3, 5, and so on. But how many primes do we need to try? In fact, we need only try the primes up to $\text{floor}(\sqrt{10\,001}) = 100$, because if 10 001 is *not* prime, then it will have at least two factors, which cannot both be strictly greater than $\sqrt{10\,001}$. Thus, we need only try the primes on the above list. It turns out that $10\,001 = 73 \times 137$, so it is not prime.

The above list is also long enough to check whether 10 007 is prime, since $\text{floor}(\sqrt{10\,007}) = 100$; this time it turns out that the number is prime.

In general, given a positive integer n, we need only test n for divisibility by prime numbers up to $\text{floor}(\sqrt{n})$ in order to check whether or not n is prime.

There are several ways to prove Fermat's Little Theorem, but perhaps the most elegant uses Corollary 3.1. Suppose first that a is a non-zero member of $\mathbb{Z}_p$. Then, by Corollary 3.1, row a of the multiplication table for $\mathbb{Z}_p$ includes all of $\mathbb{Z}_p$.

$\times_p$	0	1	2	$\cdots$	$p-1$
0	0	0	0	$\cdots$	0
1	0	1	2	$\cdots$	$p-1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
a	0	a	$\cdots$		
$\vdots$	$\vdots$	$\vdots$			$\vdots$
$p-1$	0	$p-1$	$\cdots$	$\cdots$	1

The bottom right entry in the table is 1 because

$$(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod p.$$

Therefore, the non-zero members of row a of this table are just the numbers

$$1, 2, \ldots, p-1, \tag{3.4}$$

in some order. Because this is a multiplication table, these numbers are the remainders on division by p of the products

$$a, 2a, \ldots, (p-1)a. \tag{3.5}$$

Therefore, the product of the $p-1$ numbers in (3.5) is congruent modulo p to the product of the $p-1$ numbers in (3.4):

$$a \times 2a \times \cdots \times (p-1)a \equiv 1 \times 2 \times \cdots \times (p-1) \pmod{p}.$$

This congruence can be rewritten as

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p},$$

and then again as

$$(a^{p-1}-1)(p-1)! \text{ is divisible by } p.$$

Now p is not a factor of $(p-1)!$, because p is prime, so we deduce that p *is* a factor of $a^{p-1}-1$. Thus

See Remark 1 after this proof, for a justification of this step.

$$a^{p-1} \equiv 1 \pmod{p}.$$

This is the required result for a in $\mathbb{Z}_p$, $a \neq 0$.

Finally, suppose that a is *any* positive integer which is not a multiple of p. Then b, the remainder on division of a by p, satisfies $0 < b < p$, because a is not a multiple of p. Hence, by the first part of the proof,

$$b^{p-1} \equiv 1 \pmod{p} \quad \text{so} \quad a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p},$$

since $a \equiv b \pmod{p}$. Thus the proof is complete.

Remarks

1. In the proof we used the fact that if a product xy has a prime factor p, then at least one of x, y must have factor p. This is not quite so obvious as it may seem, but can be proved as follows.

   This is also the key fact needed to prove uniqueness of prime factorisation; see the Introduction.

   Suppose that p is a factor of xy but p is *not* a factor of y. Then the remainder r of y on division by p is non-zero. Since p is prime, r has multiplicative inverse, z say, in $\mathbb{Z}_p$; that is,

   $$rz \equiv 1 \pmod{p}, \text{ so } yz \equiv 1 \pmod{p}.$$

   Hence $x(yz) \equiv x \pmod{p}$, and so x must have a factor p, because $x(yz) = (xy)z$ does.
2. It is possible that a smaller power of a than $p-1$ may be congruent to 1 modulo p. For example, if $a = 2$ and $p = 7$, then, by Fermat's Little Theorem, $2^6 \equiv 1 \pmod{7}$. In this case, however, the power 6 is not the smallest possible since $2^3 \equiv 1 \pmod{7}$ also.
3. If a is a non-zero number in $\mathbb{Z}_p$, where p is prime, then by Fermat's Little Theorem,

   $$a \times a^{p-2} \equiv a^{p-1} \equiv 1 \pmod{p}.$$

   Thus the multiplicative inverse b of a satisfies

   $$b \equiv a^{p-2} \pmod{p}.$$

   Even for large p, this formula is quite a good way to find the multiplicative inverse of a in $\mathbb{Z}_p$, as long as repeated squaring is used.

3.4 Fermat's legacy

This subsection will not be assessed.

We end this section with some remarks about Fermat's other work.

In a letter to a colleague in 1650 he summarised 'le compte de mes reveries sur le sujet des nombres' ('the account of my musing on the subject of numbers'). Amongst many results, which he stated without proof, were the following.

(1) Every prime number of the form $4n + 1$ can be written in a unique way as the sum of two squares.

For example,

$$29 = 2^2 + 5^2.$$

(2) The equation $x^3 + y^3 = z^3$ has no solution in positive integers.

(3) Every integer of the form $2^{2^n} + 1$ is prime.

For example,

$$2^{2^3} + 1 = 257 \text{ (a prime)}.$$

Fermat also described his 'method of infinite descent' for proving results of this type about positive integers. His idea was to show that if one counter-example to the result exists, then there must exist a second smaller counter-example, and hence a third yet smaller, and so on. As there cannot be infinitely many smaller counter-examples, the original counter-example could not have existed.

It is quite possible that Fermat did prove (1) and (2) by his method, but (3) was shown to be false by Euler who found the counter-example

$$2^{2^5} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417.$$

Another assertion made by Fermat was that each of the equations

$$x^n + y^n = z^n, \quad \text{where } n \geq 3,$$

has no solution in positive integers. This assertion was written in his copy of Diophantus' *Arithmetica*. Fermat wrote that he had a truly wonderful proof, but the margin was too narrow to contain it.

The Greek mathematician Diophantus is believed to have lived around 250 AD, in Alexandria. His book *Arithmetica*, a collection of problems whose solutions are positive integers, had great influence in later centuries.

During the 18th, 19th and 20th centuries, **Fermat's Last Theorem**, as his assertion came to be called, acquired increasing celebrity as a succession of eminent professional mathematicians tried and failed to solve it. Much useful number theory was discovered in the process, but the original problem remained stubbornly resistant. When a large prize was offered for a solution in 1908, many amateur mathematicians took an interest and the professionals have been inundated with alleged proofs ever since.

Fermat's Last Theorem was finally proved in 1994. The proof can be said to have begun in 1985 when a German mathematician Gerhard Frey suggested a possible link between Fermat's Last Theorem and a conjecture about so-called elliptic curves, made by the Japanese mathematicians Yutaka Taniyama and Goro Shimura in the 1950s and 1960s. In 1986, the American mathematician Kenneth Ribet showed that this conjecture does indeed imply Fermat's Last Theorem.

Elliptic curves have equations of the form

$$y^2 = x^3 + ax^2 + bx + c.$$

They are not ellipses, but they are related to ellipses.

At this point, Andrew Wiles, an English mathematician who had trained at Cambridge but worked in the United States, decided to try and prove the Shimura–Taniyama conjecture. After seven years working in secret, he announced, during a lecture in Cambridge in June 1993, that he had proved a special case of the conjecture from which Fermat's Last Theorem follows. This announcement made headlines in the world's press, but a few months later a colleague found a gap in Wiles' 200 page proof. Wiles spent a further agonising year working to fill the gap, first alone and later with Richard Taylor, an English mathematician then at Cambridge. In October 1994, when many experts had begun to feel that the gap would not be filled, two manuscripts appeared, a long one by Wiles proving the special case of the Shimura–Taniyama conjecture (and thus Fermat's Last Theorem) by a different method, and a short one by Taylor and Wiles,

containing a key step needed in the long paper. These papers were published in the prestigious journal *Annals of Mathematics*, forming the entire content of its May 1995 issue.

This proof of Fermat's Last Theorem is remarkable in that it draws on many diverse and deep areas of modern mathematics, largely developed with different purposes in mind. Parts of the proof have already been simplified, but it is very unlikely that such simplification will ever result in a proof that Fermat himself could have devised!

Summary of Section 3

In this section you have met:

- ◇ the operations $+_n$ and $\times_n$ of modular arithmetic;
- ◇ multiplicative inverses, found by Euclid's Algorithm;
- ◇ a theorem that states which members of $\mathbb{Z}_n$ have multiplicative inverses;
- ◇ Fermat's Little Theorem.

Exercises for Section 3

Exercise 3.1

Use Euclid's Algorithm to find the multiplicative inverses of

(a) 13 in $\mathbb{Z}_{30}$; (b) 25 in $\mathbb{Z}_{36}$; (c) 13 in $\mathbb{Z}_{20}$.

Exercise 3.2

Use Fermat's Little Theorem to find the remainders when

(a) 5^{26} is divided by 13; (b) 41^{41} is divided by 19.

4 Cryptography

When a sensitive message is transmitted, it is usually first transformed by applying a process called a cipher, in order that the message can be read only by those capable of reversing the cipher process. Such ciphers have been used throughout history for military and diplomatic communications, but in recent years they have been needed increasingly to protect electronic transfer of business information and money.

Taken together these are called **cryptology**.

The design of such ciphers is called **cryptography** and the process of breaking them is called **cryptanalysis**.

In this section we give a very brief indication of how number theory has contributed to these important subjects.

4.1 Additive ciphers and multiplicative ciphers

We begin by defining some basic terms associated with cryptography. A **message**, also known as **messagetext** or **plaintext**, consists of a finite sequence of characters chosen from some finite set Ω, such as the English alphabet. We define a **cipher** to be a function f with domain Ω and codomain Ω, which is one-one and so has an inverse function f^{-1} with domain Ω. We also refer to f as a **cipher on** Ω. To **encipher** a message we apply the function f to the characters of the message in turn; this produces the **ciphertext**. To **decipher** this ciphertext, we apply the inverse function f^{-1}.

For example, if

$$\Omega = \{A, B, C, \ldots, X, Y, Z\},$$

then the following function f is one-one on Ω.

$$\begin{array}{cccccccccccc} & A & B & C & D & E & \ldots & W & X & Y & Z \\ f & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow & \downarrow \\ & D & E & F & G & H & \ldots & Z & A & B & C \end{array}$$

The function f transforms each letter to the one three places after it in the alphabet (with wrap-around), and f^{-1} transforms each letter to the one three places before it (or, equivalently, 23 places after it). Thus f is a cipher, which enciphers the message 'HAPPYNEWYEAR' to give the ciphertext 'KDSSBQHZBHDU'. It is called **Caesar's cipher**, after a similar cipher used by Julius Caesar.

In order to use modular arithmetic in the design of more sophisticated ciphers, we replace letters by numbers. In the English alphabet, it is convenient to replace the 26 letters by corresponding members of $\mathbb{Z}_{26}$ as follows.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Written in $\mathbb{Z}_{26}$, the message 'HAPPYNEWYEAR' appears as the sequence:

$$\langle 8, 1, 16, 16, 25, 14, 5, 23, 25, 5, 1, 18 \rangle,$$

In this section, we use the notation $\langle \cdots \rangle$ for finite sequences of integers.

and Caesar's cipher has rule

$$f(m) = m +_{26} 3, \text{ and } f^{-1}(c) = c +_{26} 23.$$

Note that throughout this section we use m for a term of the messagetext and c for a term of the ciphertext.

Caesar's cipher is one example of the family of *additive ciphers* on the set $\mathbb{Z}_n$, defined as follows.

Definition

Let n be a positive integer and let k be in $\mathbb{Z}_n$, with $k \neq 0$. The **additive cipher** A_k on $\mathbb{Z}_n$ has rule

$$A_k(m) = m +_n k.$$

Thus A_k has domain $\mathbb{Z}_n$.

Moreover, it can be shown that A_k^{-1} has rule

$$A_k^{-1}(c) = c +_n k',$$

where k' is in $\mathbb{Z}_n$ with $k + k' = n$.

(We have included a result in the definition box so that the rules for A_k and A_k^{-1} are in one place.)

In Caesar's cipher we have $n = 26$, $k = 3$ and $k' = 23$. When a family of ciphers depends on a parameter k in this way, the parameter is called the **key**. Although a given fixed additive cipher would not be very secure, considerably more security could be achieved by refinements such as the following:

- ◇ letting the key vary through the message in some complicated way, known to both the encipherer and the decipherer;
- ◇ splitting the message into blocks of d characters in $\mathbb{Z}_n$, transforming each block $\langle m_0, m_1, m_2, \ldots, m_{d-1}\rangle$ by a one-one function such as
$\langle m_0, m_1, m_2, \ldots, m_{d-1}\rangle \longmapsto m_0 + m_1 \times n + m_2 \times n^2 + \cdots + m_{d-1} \times n^{d-1}$
into an integer in $\mathbb{Z}_N$, where $N = n^d$, and then using an additive cipher on $\mathbb{Z}_N$.

We shall ignore such refinements and methods of breaking ciphers. We concentrate on defining families of ciphers, using modular arithmetic, which are likely to be intrinsically better than additive ciphers. Our model for such ciphers is shown in the diagram below.

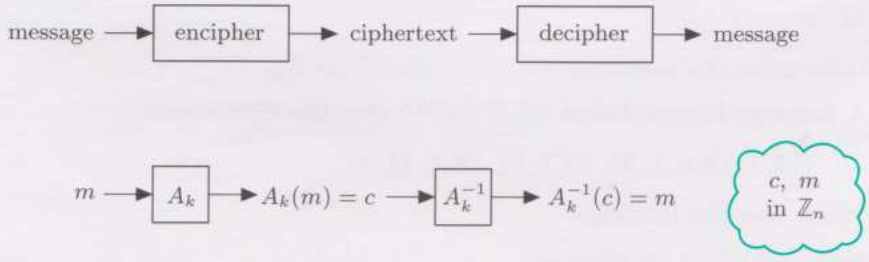


Figure 4.1

Another family of ciphers on $\mathbb{Z}_n$ which are easy to implement are the so-called *multiplicative ciphers*.

Definition

Let n be a positive integer and let k in $\mathbb{Z}_n$ be coprime with n. The **multiplicative cipher** M_k on $\mathbb{Z}_n$ has rule

$$M_k(m) = k \times_n m.$$

Moreover, it can be shown that M_k^{-1} has rule

$$M_k^{-1}(c) = k' \times_n c,$$

where k' is the multiplicative inverse of k in $\mathbb{Z}_n$.

Thus M_k^{-1} is the multiplicative cipher $M_{k'}$.

We know that k has a multiplicative inverse k' in $\mathbb{Z}_n$, by Lemma 3.1, since k and n are coprime. Moreover, by Theorem 3.1, row k of the multiplication table for $\mathbb{Z}_n$ includes each member of $\mathbb{Z}_n$ exactly once. Since this row is the image set of M_k, it follows that M_k is one-one. The rule for its inverse function follows from the fact that if $c = k \times_n m$, then

$$k' \times_n c = k' \times_n (k \times_n m) = 1 \times_n m = m.$$

Taking $n = 26$ and $k = 9$, we obtain the cipher

$$M_9(m) = 9 \times_{26} m,$$

which enciphers our 'HAPPYNEWYEAR' message as follows.

	8	1	16	16	25	14	5	23	25	5	1	18	(message)
M_9	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	
	20	9	14	14	17	22	19	25	17	19	9	6	(ciphertext)

For example,

$$9 \times 8 \equiv 20 \pmod{26}.$$

To decipher the ciphertext we need to apply the inverse function M_9^{-1}. Since 9 has multiplicative inverse 3 in $\mathbb{Z}_{26}$, we have $M_9^{-1} = M_3$. For example, the first character of the ciphertext above is $c = 20$, and

$$M_9^{-1}(20) = M_3(20) = 3 \times_{26} 20 = 8,$$

because $60 \equiv 8 \pmod{26}$. This is indeed the first character of the message.

Activity 4.1 Multiplicative ciphers

A multiplicative cipher on $\mathbb{Z}_{26}$ is defined by the function

$$M_7(m) = 7 \times_{26} m.$$

Note that 26 and 7 *are* coprime.

(a) Determine the multiplicative inverse of 7 in $\mathbb{Z}_{26}$.

(b) A message is enciphered using M_7 to give the ciphertext:

$$\langle 10, 1, 14, 9, 1, 22, 20, 1, 10, 10, 1, 14, 9 \rangle.$$

What was the message?

Solutions are given on page 44.

4.2 Exponential ciphers and RSA ciphers

Additive and multiplicative ciphers both have the serious disadvantage that if a cryptanalyst can obtain a small amount of messagetext and its corresponding ciphertext, then the key can easily be found.

Our next family of ciphers does a better job of concealing its key. These ciphers are defined on sets $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, where p is a prime number. For example, we might use $p = 29$, so that $0, 1, \ldots, 25$ could represent the English alphabet as before.

Definition

Let p be a prime number and let k in $\mathbb{Z}_{p-1}$ be coprime with $p-1$. The **exponential cipher** E_k on $\mathbb{Z}_p$ has rule

$$E_k(m) \equiv m^k \pmod{p}.$$

Moreover, it can be shown that E_k^{-1} has rule

$$E_k^{-1}(c) \equiv c^{k'} \pmod{p},$$

where k' is the multiplicative inverse of k in $\mathbb{Z}_{p-1}$.

This *congruence* defines $E_k(m)$ uniquely since we want $E_k(m)$ to lie in $\mathbb{Z}_p$.

At first sight it is not at all clear that this function E_k is one-one, nor that $E_k^{-1} = E_{k'}$, but we shall see that this is the case. First, however, we look at an exponential cipher in action. Take $p = 29$ and choose the key $k \in \mathbb{Z}_{28}$ so that k and $p - 1 = 28$ are coprime; for example, take $k = 5$. If $m = 2$ is a term of the message, then $E_k(m)$ is

$$\begin{aligned} E_5(2) &\equiv 2^5 \pmod{29} \\ &\equiv 32 \pmod{29} \\ &\equiv 3 \pmod{29}. \end{aligned}$$

Thus the corresponding term of the ciphertext is $c = 3$.

To decipher, we apply the inverse function E_5^{-1}. The multiplicative inverse of 5 in $\mathbb{Z}_{28}$ is 17, so $E_5^{-1} = E_{17}$. We can evaluate $c^{17} \equiv 3^{17} \pmod{29}$ using the repeated squares technique.

$5 \times 17 = 85 = 3 \times 28 + 1.$

3^{2^n}	3^1	3^2	3^4	3^8	3^{16}
$3^{2^n} \pmod{29}$	3	9	23	7	20

See Subsection 1.3. Note the following shortcut:

$$23^2 \equiv (-6)^2 \equiv 7 \pmod{29}.$$

We obtain

$$c^{17} \equiv 3^{17} \equiv 3 \times 3^{16} \equiv 3 \times 20 \equiv 60 \equiv 2 \pmod{29},$$

giving $m = 2$, as expected.

To prove that E_k is one-one and that $E_k^{-1} = E_{k'}$ is tricky. It is sufficient to show that if m is in $\mathbb{Z}_p$ and $c \equiv m^k \pmod{p}$, then $c^{k'} \equiv m \pmod{p}$. If $c \equiv m^k \pmod{p}$, then we have

$$c^{k'} \equiv (m^k)^{k'} \equiv m^{kk'} \pmod{p}.$$

Since k' is the multiplicative inverse of k in $\mathbb{Z}_{p-1}$, there is an integer l such that $kk' = l(p-1) + 1$, and so

$$m^{kk'} = m^{l(p-1)+1} = (m^{p-1})^l m.$$

If $m \neq 0$, then m is a positive integer in $\mathbb{Z}_p$ and so is not a multiple of p. Hence Fermat's Little Theorem implies that $m^{p-1} \equiv 1 \pmod{p}$, which gives

$$m^{kk'} \equiv m \pmod{p},$$

a congruence which also holds when $m = 0$. Thus

$$c^{k'} \equiv m^{kk'} \equiv m \pmod{p},$$

as required.

Activity 4.2 Deciphering an exponential cipher

An exponential cipher is defined on $\mathbb{Z}_{29}$ by

$$E_3(m) \equiv m^3 \pmod{29}.$$

(a) Determine the multiplicative inverse of 3 in $\mathbb{Z}_{28}$.

(b) A message was enciphered using E_3 to give the ciphertext

$$\langle 8, 9 \rangle.$$

What was the message?

Solutions are given on page 44.

To see why an exponential cipher is better than an additive or multiplicative one, imagine that a cryptanalyst knows that m is enciphered to c by an exponential cipher:

$$c \equiv E_k(m) \equiv m^k \pmod{p}, \tag{4.1}$$

where the key k is coprime with $p - 1$. The problem is to find k, given congruence (4.1). For small values of p, the key can be found by checking all possible values of k, but for larger values of p the problem is much harder, and certainly very much harder than the corresponding enciphering calculations. When congruence (4.1) holds, k is called the **discrete logarithm** of c with base m and modulus p, and, as you may imagine, the problem of computing discrete logarithms has received much attention from number theorists and cryptographers.

Finally, we describe the RSA ciphers, so-called because they were invented by R. L. Rivest, A. Shamir and L. Adleman, in 1977. These ciphers are defined on sets of the form $\mathbb{Z}_{pq} = \{0, 1, 2, \ldots, pq - 1\}$, where p and q are prime numbers. For example, we might use $p = 5$ and $q = 11$, so that $0, 1, \ldots, 25$ could represent the English alphabet as before.

Much larger prime numbers are used in practice, together with the blocking technique described in Subsection 4.1, but here we are deliberately keeping the numbers small.

Definition

Let p and q be prime numbers and let k in $\mathbb{Z}_{(p-1)(q-1)}$ be coprime with $(p-1)(q-1)$. The **RSA cipher** R_k on $\mathbb{Z}_{pq}$ has rule

$$R_k(m) \equiv m^k \pmod{pq}.$$

Moreover, it can be shown that R_k^{-1} has rule

$$R_k^{-1}(c) \equiv c^{k'} \pmod{pq},$$

where k' is the multiplicative inverse of k in $\mathbb{Z}_{(p-1)(q-1)}$.

Once again, it is not obvious that the function R_k is one-one, nor that $R_k^{-1} = R_{k'}$, but we shall see that this is the case. First, however, we look at an RSA cipher in action. Take $p = 5$, $q = 11$ and choose the key $k \in \mathbb{Z}_{40}$ so that k and $(p-1)(q-1) = 40$ are coprime. For example, take $k = 7$.

If $m = 8$ is a term of the message, then $R_k(m)$ is

$$R_7(8) \equiv 8^7 \pmod{55}.$$

Using repeated squaring, we obtain

8^{2^n}	8^1	8^2	8^4
$8^{2^n} \pmod{55}$	8	9	26

and so

$$R_7(8) \equiv 8^7 \equiv 8^1 \times 8^2 \times 8^4 \equiv 8 \times 9 \times 26 \equiv 2 \pmod{55}.$$

Thus the corresponding term of the ciphertext is $c = 2$.

To decipher, we apply the inverse function R_7^{-1}. The multiplicative inverse of 7 in $\mathbb{Z}_{40}$, is 23, so $R_7^{-1} = R_{23}$. We can evaluate $c^{23} \equiv 2^{23} \pmod{55}$ using the following table.

$7 \times 23 = 161 = 4 \times 40 + 1$

2^{2^n}	2^1	2^2	2^4	2^8	2^{16}
$2^{2^n} \pmod{55}$	2	4	16	36	31

We obtain

$$2^{23} \equiv 2^1 \times 2^2 \times 2^4 \times 2^{16} \equiv 2 \times 4 \times 16 \times 31 \equiv 18 \times 31 \equiv 8 \pmod{55},$$

giving $m = 8$, as expected.

To prove that R_k is one-one and that $R_k^{-1} = R_{k'}$ is again tricky. It is sufficient to show that if m is in $\mathbb{Z}_{pq}$ and $c \equiv m^k \pmod{pq}$, then $c^{k'} \equiv m \pmod{pq}$. If $c \equiv m^k \pmod{pq}$, then we have

$$c^{k'} \equiv (m^k)^{k'} \equiv m^{kk'} \pmod{pq}.$$

Since k' is the multiplicative inverse of k in $\mathbb{Z}_{(p-1)(q-1)}$, there is an integer l such that $kk' = l(p-1)(q-1) + 1$, and so

$$m^{kk'} = m^{l(p-1)(q-1)+1} = (m^{p-1})^{l(q-1)} m.$$

If m is not a multiple of p, then Fermat's Little Theorem implies that $m^{p-1} \equiv 1 \pmod{p}$, which gives

Thus, in particular, $m \neq 0$.

$$m^{kk'} \equiv m \pmod{p},$$

a congruence which also holds if m is a multiple of p (including the zero multiple). Similarly,

$$m^{kk'} \equiv m \pmod{q}.$$

Hence $m^{kk'} - m$ is divisible by p and by q, and so by their product pq, since p and q are primes. Thus

This follows by Remark 1 on page 29.

$$c^{k'} \equiv m^{kk'} \equiv m \pmod{pq},$$

as required.

Activity 4.3 Deciphering an RSA cipher

An RSA cipher is defined on $\mathbb{Z}_{55}$ by

$$R_{27}(m) \equiv m^{27} \pmod{55}.$$

(a) Determine the multiplicative inverse of 27 in $\mathbb{Z}_{40}$.

(b) A message was enciphered by R_{27} to give the ciphertext

$$\langle 9, 5 \rangle.$$

What was the message?

Solutions are given on page 44.

The remainder of this section will not be assessed.

The calculations above do not indicate why RSA ciphers are so significant. Notice, however, that in order to apply the formula $R_k(m) \equiv m^k \pmod{pq}$ the encipherer needs to know the values of the product pq and the exponent k, but does not need to know the values of p and q. Indeed, for large primes p and q it may be extremely difficult to factorise pq, taking years of computer effort if pq is, say, several hundred digits long. Thus the encipherer will be unable to find p and q, except by luck, and so unable to find k' which is needed for deciphering. On the other hand, the calculations involved in *using* an RSA cipher with such large numbers are feasible on suitably programmed machines.

All this means that a person P, who wishes to receive enciphered messages that cannot be deciphered by anyone else, can choose large primes p and q, find k with multiplicative inverse k' in $\mathbb{Z}_{(p-1)(q-1)}$ using Euclid's algorithm, and then *make public* the values of k and the product $N = pq$. To encipher a message to P, any other person represents their message as a sequence of (large) integers in $\mathbb{Z}_N$, by using the blocking technique described earlier in this section, and then enciphers these integers with the function defined by

$$R_k(m) \equiv m^k \pmod{N},$$

evaluated by the repeated squares method. Only P knows the value of k', so only P can decipher such messages using $R_k^{-1} = R_{k'}$.

The RSA cipher is an example of a so-called **public-key cipher**, for which the enciphering process can be made public without betraying the deciphering process. The existence of such ciphers creates the possibility of each person (and each organisation) publishing their own RSA cipher, which can be used to send them private messages, funds, and so on.

This possibility raises many issues of great significance, not least of which is the displeasure of governments, who may prefer to be able to monitor the activities of their citizens while keeping their own activities 'secure'. Indeed, there has already been controversy about the publication of certain public-key ciphers. On the other hand, there is a great incentive to researchers in number theory to find ever better algorithms to factorise large numbers, in order to facilitate the breaking of RSA ciphers. There is even the possibility that a more efficient algorithm may be found to decipher an RSA cipher, *without* the need for factorisation. Anyone finding such an algorithm should expect a large amount of interest to be shown in their work!

Summary of Section 4

In this section you have seen how number theory plays an unexpected role in modern methods of cryptography.

Exercises for Section 4

Exercise 4.1

Decipher each of the following pieces of ciphertext.

(a) $\langle 15, 28, 5, 2 \rangle$, which was enciphered using the multiplicative cipher $M_{13}(m) \equiv 13 \times_{30} m$ on $\mathbb{Z}_{30}$.

(b) $\langle 25, 13, 19 \rangle$, which was enciphered using the exponential cipher $E_{25}(m) \equiv m^{25} \pmod{37}$ on $\mathbb{Z}_{37}$.

(c) $\langle 26, 30, 4, 12, 9, 24, 26 \rangle$, which was enciphered using the RSA cipher $R_{13}(m) \equiv m^{13} \pmod{33}$ on $\mathbb{Z}_{33}$.

In each case the English alphabet is represented as follows.

A	B	C	...	X	Y	Z
1	2	3	...	24	25	26

Note that the multiplicative inverses needed for this exercise were all calculated in Exercise 3.1.

5 Number theory and Mathcad

In this section, you have the opportunity to develop your understanding of the concepts in this chapter, to check some of your earlier calculations, and also to try out the methods with much larger numbers than your calculator can handle.

The computing work for this chapter uses Mathcad to:

- ◇ calculate the quotient and remainder in the Division Algorithm;
- ◇ calculate the remainders on division by n of a sequence of powers a^k, $k = 1, 2, \ldots$;
- ◇ calculate the remainders on division by n of a power a^k using the repeated squaring algorithm;
- ◇ generate addition and multiplication tables for $\mathbb{Z}_n$;
- ◇ calculate multiplicative inverses, using Euclid's Algorithm;
- ◇ factorise large numbers and also multiply large numbers.

Refer to Computer Book D for the work in this section.

Summary of Chapter D2

In this chapter you acquired some techniques of number theory and applied some of its basic results. In particular you have seen the application of Fermat's Little Theorem in cryptography.

Learning outcomes

You have been working towards the following learning outcomes.

Terms to know and use

Division Algorithm, quotient, remainder, divisible by n, divisor, factor, congruent modulo n, congruence, modulus, digit sum, alternating digit sum, common factor, coprime, multiplicative inverse, Euclid's Algorithm, cipher, messagetext, ciphertext, additive cipher, key, multiplicative cipher, exponential cipher, RSA cipher.

Terms to be aware of

Theorem, lemma, corollary, counter-example, commutative operation, associative operation, star polygon, cryptography, cryptanalyst, encipher, decipher, Caesar's cipher, discrete logarithm, public-key cipher.

Notation to know and use

$a \equiv b \pmod{n}$, $a \not\equiv b \pmod{n}$, $a \equiv b \equiv c \pmod{n}$, $\mathbb{Z}_n$, $+_n$, $\times_n$.

Mathematical skills

- ◇ Apply the Division Algorithm (Theorem 1.1).
- ◇ Follow the use of Properties of Congruence (Theorem 1.2).
- ◇ Find remainders on division of large numbers by:

  $3, 9, 11;\ 2, 4, 8, \ldots;\ 6, 12;\ 7, 13.$
- ◇ Construct tables for $+_n$ and $\times_n$ for $\mathbb{Z}_n$, and describe patterns therein.
- ◇ Use Euclid's Algorithm to find the multiplicative inverse of an element in $\mathbb{Z}_n$.
- ◇ Follow the development of Theorem 3.1.
- ◇ Use Fermat's Little Theorem (Theorem 3.2) to find remainders of powers modulo p.
- ◇ Use additive, multiplicative, exponential and RSA ciphers to encipher a message and to decipher a ciphertext.

Solutions to Activities

Solution 1.1

There is no need to use $q = \text{floor}(a/n)$ if you can 'see' how the division of a by n works out.

(a) Here $77 = 8 \times 9 + 5$, so

$$q = 8 \quad \text{and} \quad r = 5.$$

(b) Here

$$q = \text{floor}(-100/11) = \text{floor}(-9.0909\ldots) = -10,$$

so

$$r = -100 - (-10) \times 11 = 10.$$

(c) Here

$$q = \text{floor}(987\,654\,321/8) = \text{floor}(123\,456\,790.1\ldots) = 123\,456\,790,$$

so

$$r = 987\,654\,321 - 123\,456\,790 \times 8 = 1.$$

Solution 1.3

We can write

$$a = pn + r,$$

where p and r are integers with $0 \leq r < n$.

Since $a - b$ is a multiple of n, we can write

$$a - b = kn,$$

where k is an integer.

Eliminating a from these equations, we obtain

$$b = a - kn = (pn + r) - kn = (p - k)n + r.$$

Because $p - k$ is an integer, it follows from the Division Algorithm that b also has remainder r on division by n.

Solution 1.4

(a) True (b) False (c) True

(d) True (e) True (f) True

Solution 1.5

Since equations (1.2) hold, we deduce, by subtraction, that

$$(a - b) - (c - d) = kn - ln,$$

that is,

$$(a - c) - (b - d) = (k - l)n,$$

and this implies that $a - c \equiv b - d \pmod{n}$, since $k - l$ is an integer.

Solution 1.7

We obtain

$$15^1 \equiv 15 \pmod{55},$$
$$15^2 \equiv 225 \equiv 5 \pmod{55},$$
$$15^4 \equiv 5^2 \equiv 25 \pmod{55},$$
$$15^8 \equiv 25^2 \equiv 20 \pmod{55},$$
$$15^{16} \equiv 20^2 \equiv 15 \pmod{55}.$$

Since $19 = 1 + 2 + 16$, we obtain

$$\begin{aligned} 15^{19} &\equiv 15^1 \times 15^2 \times 15^{16} \pmod{55} \\ &\equiv 15 \times 5 \times 15 \pmod{55} \\ &\equiv 1125 \equiv 25 \pmod{55}, \end{aligned}$$

as required.

Solution 2.5

(a) This number is divisible by 2 and, from Activity 2.1, is congruent to 2 modulo 3. Hence, by congruence (2.2), $r_6 \equiv -4 \pmod{6}$, so the remainder on division by 6 is $r_6 = 2$.

(b) This number is congruent to 2 modulo 3 and, from Activity 2.4, is divisible by 4. Hence, by congruence (2.3), $r_{12} \equiv 8 \pmod{12}$, so the remainder on division by 12, is $r_{12} = 8$.

Solution 2.7

(a) On division by 7, the remainders are:

6	341	723	110	832	864	
6	5	2	5	6	3	(mod 7)

and their alternating sum is

$$3 - 6 + 5 - 2 + 5 - 6 = -1.$$

Hence the number is congruent to -1 modulo 7, and so gives remainder 6 on division by 7.

(b) On division by 13, the remainders are:

6	341	723	110	832	864	
6	3	8	6	0	6	(mod 13)

and their alternating sum is

$$6 - 0 + 6 - 8 + 3 - 6 = 1.$$

Hence the number gives remainder 1 on division by 13.

Solution 3.1

(a) 3, 1, 4, 6, 2

(b) 1, 0, 3, 2, 4

Solution 3.2

(a)

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(b) The most striking pattern is that each row is obtained from the one above by shifting the entries one place to the left, moving entries which drop off the left end to the right end. In particular, the entries in each 'uphill' diagonal of a table are constant.

This pattern arises because if you increase the row number by 1 and decrease the column number by 1, then the corresponding sum remains the same.

One consequence of this pattern is that the addition table is symmetric under reflection in its main 'downhill' diagonal. This symmetry of the table reflects the fact that, for all a and b in $\mathbb{Z}_n$,

$$a + b = b + a,$$

so

$$a +_n b = b +_n a.$$

Solution 3.3

(a)

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b) There seems to be no striking overall pattern of the type seen in the addition tables.

However they are symmetric under a reflection in the main 'downhill' diagonal because, for all a, b in $\mathbb{Z}_n$,

$$a \times b = b \times a,$$

so

$$a \times_n b = b \times_n a.$$

(There are other symmetries of the tables obtained by omitting row 0 and column 0, which you may like to investigate.)

(c) It appears that a non-zero row (or column) of the multiplication table for $\mathbb{Z}_n$ includes all the numbers from $\mathbb{Z}_n$ if and only if the row (or column) number has no factors in common with n, other than 1. For example, in the table for $\mathbb{Z}_6$, rows 1 and 5 include all of $\mathbb{Z}_6$, but the other rows do not.

Solution 3.4

Using the definition of $+_n$ and Theorem 1.2(d), we obtain

$$\begin{aligned} a +_n (b +_n c) &\equiv a + (b +_n c) \pmod{n} \\ &\equiv a + (b + c) \pmod{n}. \end{aligned}$$

Similarly,

$$(a +_n b) +_n c \equiv (a + b) + c \pmod{n},$$

and so the associativity of $+_n$ follows from that of ordinary addition: $a + (b + c) = (a + b) + c$.

Solution 3.5

(a) 1, 2, 4, 5, 7 and 8 are coprime with 9.

(b) The multiplication table for $\mathbb{Z}_9$ confirms that rows 1, 2, 4, 5, 7 and 8 include the whole of $\mathbb{Z}_9$, whereas rows 0, 3 and 6 do not.

	$\times_9$	0	1	2	3	4	5	6	7	8
	0	0	0	0	0	0	0	0	0	0
→	1	0	1	2	3	4	5	6	7	8
→	2	0	2	4	6	8	1	3	5	7
	3	0	3	6	0	3	6	0	3	6
→	4	0	4	8	3	7	2	6	1	5
→	5	0	5	1	6	2	7	3	8	4
	6	0	6	3	0	6	3	0	6	3
→	7	0	7	5	3	1	8	6	4	2
→	8	0	8	7	6	5	4	3	2	1

Solution 3.6

(a) Using the Division Algorithm repeatedly (until remainder 1 appears):

$$\begin{aligned} 12 &= 1 \times 7 + 5 \\ 7 &= 1 \times 5 + 2 \\ 5 &= 2 \times 2 + 1. \end{aligned}$$

Eliminating multiples of 2 and 5:

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2(7 - 1 \times 5) \\ &= -2 \times 7 + 3 \times 5 \\ &= -2 \times 7 + 3(12 - 1 \times 7) \\ &= 3 \times 12 - 5 \times 7. \end{aligned}$$

Hence

$$7 \times (-5) = 12 \times (-3) + 1,$$

so $7 \times (-5) \equiv 1 \pmod{12}$, and thus the multiplicative inverse of 7 in $\mathbb{Z}_{12}$ is $-5 + 12 = 7$.

(b) Using the Division Algorithm repeatedly:

$$\begin{aligned} 26 &= 2 \times 9 + 8 \\ 9 &= 1 \times 8 + 1. \end{aligned}$$

Eliminating multiples of 8:

$$\begin{aligned} 1 &= 9 - 1 \times 8 \\ &= 9 - 1 \times (26 - 2 \times 9) \\ &= -1 \times 26 + 3 \times 9. \end{aligned}$$

Hence

$$3 \times 9 = 1 \times 26 + 1,$$

so $3 \times 9 \equiv 1 \pmod{26}$, and thus the multiplicative inverse of 9 in $\mathbb{Z}_{26}$ is 3.

Solution 3.7

(a) By Fermat's Little Theorem, with $p = 19$ and $a = 3$, we know that $3^{18} \equiv 1 \pmod{19}$. Hence the remainder is 1.

(b) By (a) and Theorem 1.2,

$$3^{55} \equiv 3^{18\times 3+1} \equiv (3^{18})^3 \times 3 \equiv 1^3 \times 3 \equiv 3 \pmod{19}.$$

Hence the remainder is 3.

(c) First $16 \equiv 5 \pmod{11}$, so $16^{103} \equiv 5^{103} \pmod{11}$. By Fermat's Little Theorem, with $p = 11$ and $a = 5$, we know that $5^{10} \equiv 1 \pmod{11}$. Therefore

$$\begin{aligned} 16^{103} \equiv 5^{103} &\equiv (5^{10})^{10} \times 5^3 \\ &\equiv 1 \times 125 \equiv 4 \pmod{11}. \end{aligned}$$

Hence the remainder is 4.

Solution 4.1

(a) Using the Division Algorithm repeatedly:

$$\begin{aligned} 26 &= 3 \times 7 + 5 \\ 7 &= 1 \times 5 + 2 \\ 5 &= 2 \times 2 + 1. \end{aligned}$$

Eliminating multiples of 2 and 5:

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ &= 5 - 2(7 - 1 \times 5) \\ &= -2 \times 7 + 3 \times 5 \\ &= -2 \times 7 + 3(26 - 3 \times 7) \\ &= 3 \times 26 - 11 \times 7. \end{aligned}$$

Hence

$$-11 \times 7 = -3 \times 26 + 1,$$

and since $-11 \equiv 15 \pmod{26}$, the multiplicative inverse of 7 in $\mathbb{Z}_{26}$ is 15.

(b) The message is deciphered by applying $M_7^{-1}(c) = M_{15}(c) = 15 \times_{26} c$. Thus we need to find

$$\begin{aligned} M_{15}(10) &= 15 \times_{26} 10 = 20, \\ M_{15}(1) &= 15 \times_{26} 1 = 15, \\ M_{15}(14) &= 15 \times_{26} 14 = 2, \\ M_{15}(9) &= 15 \times_{26} 9 = 5, \\ M_{15}(22) &= 15 \times_{26} 22 = 18, \\ M_{15}(20) &= 15 \times_{26} 20 = 14. \end{aligned}$$

Hence the messagetext is

$$\langle 20, 15, 2, 5, 15, 18, 14, 15, 20, 20, 15, 2, 5\rangle.$$

This represents

'TOBEORNOTTOBE'

in the English alphabet.

Solution 4.2

(a) Since $28 = 9 \times 3 + 1$, we have

$$-9 \times 3 = -1 \times 28 + 1,$$

so

$$-9 \times 3 \equiv 1 \pmod{28}$$

and hence $-9 + 28 = 19$ is the multiplicative inverse of 3 in $\mathbb{Z}_{28}$.

(b) To decipher the message we find $E_{19}(8)$ and $E_{19}(9)$. Since

8^{2^n}	8^1	8^2	8^4	8^8	8^{16}
$8^{2^n} \pmod{29}$	8	6	7	20	23

we obtain

$$8^{19} \equiv 8^1 \times 8^2 \times 8^{16} \equiv 8 \times 6 \times 23 \equiv 2 \pmod{29},$$

so $E_{19}(8) = 2$. Similarly

9^{2^n}	9^1	9^2	9^4	9^8	9^{16}
$9^{2^n} \pmod{29}$	9	23	7	20	23

gives

$$9^{19} \equiv 9^1 \times 9^2 \times 9^{16} \equiv 9 \times 23 \times 23 \equiv 5 \pmod{29},$$

so $E_{19}(9) = 5$. Hence the deciphered message is $\langle 2, 5\rangle$, which would represent 'BE' in the English alphabet.

Solution 4.3

(a) Using the Division Algorithm repeatedly:

$$\begin{aligned} 40 &= 1 \times 27 + 13 \\ 27 &= 2 \times 13 + 1. \end{aligned}$$

Eliminating the multiple of 13:

$$\begin{aligned} 1 &= 27 - 2 \times 13 \\ &= 27 - 2(40 - 1 \times 27) \\ &= -2 \times 40 + 3 \times 27. \end{aligned}$$

Hence $3 \times 27 = 2 \times 40 + 1$, so the multiplicative inverse of 27 in $\mathbb{Z}_{40}$ is 3.

(b) To decipher the message, we find $R_3(9)$ and $R_3(5)$:

$$9^3 \equiv 729 \equiv 14 \pmod{55}$$

and

$$5^3 \equiv 125 \equiv 15 \pmod{55}.$$

Hence the deciphered message is $\langle 14, 15\rangle$, which would represent 'NO' in the English alphabet.

Solutions to Exercises

Solution 1.1

(a) Repeated multiplication by 4 gives the following table.

4^n	4^0	4^1	4^2	4^3	4^4	4^5
$4^n \pmod{11}$	1	4	5	9	3	1

Hence

$$4^k \equiv 1 \pmod{11}, \text{ whenever } k \text{ is a multiple of 5,}$$

so

$$4^{12} \equiv 4^2 \times 4^{10} \equiv 5 \times 1 \equiv 5 \pmod{11}.$$

Thus the remainder is 5.

(b) Repeated multiplication by 8 gives the following table.

8^n	8^0	8^1	8^2	8^3	8^4	8^5	8^6
$8^n \pmod{25}$	1	8	14	12	21	18	19

8^7	8^8	8^9	8^{10}
2	16	3	24

Thus the remainder is 24.

(Note the possible shortcut here:

$$8^{10} \equiv 8^5 \times 8^5 \equiv 18 \times 18 \equiv 324 \equiv 24 \pmod{25}.)$$

Solution 1.2

(a) Repeated squaring gives

4^{2^n}	4^1	4^2	4^4	4^8
$4^{2^n} \pmod{11}$	4	5	3	9

so

$$4^{12} \equiv 4^4 \times 4^8 \equiv 3 \times 9 \equiv 27 \equiv 5 \pmod{11}.$$

As expected, the remainder is 5.

(b) Repeated squaring gives

8^{2^n}	8^1	8^2	8^4	8^8
$8^{2^n} \pmod{25}$	8	14	21	16

so

$$8^{10} \equiv 8^2 \times 8^8 \equiv 14 \times 16 \equiv 224 \equiv 24 \pmod{25}.$$

As expected, the remainder is 24.

Solution 2.1

In each case, the positive integer a has the same remainder as that of its final digit. These remainders are the same because the difference between a and its final digit is divisible by each of 2, 5 and 10. (For example, $112\,973 - 3 = 112\,970$, which is divisible by 2, 5 and 10.)

Solution 2.2

In each case, we use r_n to denote the remainder on division by n.

(a) $r_2 = 1$

(b) The digit sum is $53 = 17 \times 3 + 2$, so $r_3 = 2$.

(c) The number formed from the last two digits is 53, and $53 = 13 \times 4 + 1$, so $r_4 = 1$.

(d) $r_5 = 3$

(e) $r_6 \equiv 3r_2 - 2r_3 \equiv 3 - 4 \equiv -1 \pmod{6}$, so $r_6 = 5$.

(f) The required remainders are as follows.

5	230	612	009	721	753	
5	6	3	2	0	4	(mod 7)

Hence $r_7 \equiv 4 - 0 + 2 - 3 + 6 - 5 \equiv 4 \pmod{7}$, so $r_7 = 4$.

(g) The number formed from the last 3 digits is 753, and $753 = 94 \times 8 + 1$, so $r_8 = 1$.

(h) The digit sum is $53 = 5 \times 9 + 8$, so $r_9 = 8$.

(i) $r_{10} = 3$

(j) The alternating digit sum is $24 - 29 = -5$, so $r_{11} = 6$.

(k) $r_{12} \equiv 4r_3 - 3r_4 \equiv 8 - 3 \equiv 5 \pmod{12}$, so $r_{12} = 5$.

Solution 2.3

(a) If a has remainder r_2 on division by 2 and r_7 on division by 7, then

$$a = 2q_2 + r_2 \quad \text{and} \quad a = 7q_7 + r_7,$$

where q_2 and q_7 are the respective quotients. We now manipulate these two equations to obtain a on the left-hand side and multiples of q_2 and q_7 which are divisible by 14 on the right-hand side:

$$\begin{aligned} a &= 7a - 6a \\ &= 7(2q_2 + r_2) - 6(7q_7 + r_7) \\ &= (14q_2 - 42q_7) + (7r_2 - 6r_7) \\ &= 14(q_2 - 3q_7) + (7r_2 - 6r_7). \end{aligned}$$

Thus $a \equiv 7r_2 - 6r_7 \pmod{14}$, and hence

$$r_{14} \equiv 7r_2 - 6r_7 \pmod{14}.$$

(b) In Exercise 2.2, $r_2 = 1$ and $r_7 = 4$, so

$$r_{14} \equiv 7 \times 1 - 6 \times 4 \equiv -17 \pmod{14},$$

so $r_{14} = 11$.

Solution 3.1

(a) Using the Division Algorithm repeatedly:

$$30 = 2 \times 13 + 4$$
$$13 = 3 \times 4 + 1.$$

Eliminating multiples of 4:

$$\begin{aligned} 1 &= 13 - 3 \times 4 \\ &= 13 - 3(30 - 2 \times 13) \\ &= 7 \times 13 - 3 \times 30. \end{aligned}$$

Hence $7 \times 13 = 3 \times 30 + 1$, so the multiplicative inverse of 13 in $\mathbb{Z}_{30}$ is 7.

(b) Using the Division Algorithm repeatedly:

$$36 = 1 \times 25 + 11$$
$$25 = 2 \times 11 + 3$$
$$11 = 3 \times 3 + 2$$
$$3 = 1 \times 2 + 1.$$

Eliminating multiples of 2, 3 and 11:

$$\begin{aligned} 1 &= 3 - 1 \times 2 \\ &= 3 - (11 - 3 \times 3) \\ &= -11 + 4 \times 3 \\ &= -11 + 4(25 - 2 \times 11) \\ &= 4 \times 25 - 9 \times 11 \\ &= 4 \times 25 - 9(36 - 1 \times 25) \\ &= -9 \times 36 + 13 \times 25. \end{aligned}$$

Hence $13 \times 25 = 9 \times 36 + 1$, so the multiplicative inverse of 25 in $\mathbb{Z}_{36}$ is 13.

(c) Using the Division Algorithm repeatedly:

$$20 = 1 \times 13 + 7$$
$$13 = 1 \times 7 + 6$$
$$7 = 1 \times 6 + 1.$$

Eliminating multiples of 6 and 7:

$$\begin{aligned} 1 &= 7 - 1 \times 6 \\ &= 7 - (13 - 1 \times 7) \\ &= -13 + 2 \times 7 \\ &= -13 + 2(20 - 1 \times 13) \\ &= -3 \times 13 + 2 \times 20. \end{aligned}$$

Hence $-3 \times 13 = -2 \times 20 + 1$, and since $-3 \equiv 17 \pmod{20}$, the multiplicative inverse of 13 in $\mathbb{Z}_{20}$ is 17.

Solution 3.2

(a) By Fermat's Little Theorem, $5^{12} \equiv 1 \pmod{13}$, so

$$5^{26} \equiv (5^{12})^2 \times 5^2 \equiv 25 \equiv 12 \pmod{13}.$$

Hence the remainder is 12.

(b) First $41 \equiv 3 \pmod{19}$, so $41^{41} \equiv 3^{41} \pmod{19}$. By Fermat's Little Theorem, $3^{18} \equiv 1 \pmod{19}$, so

$$\begin{aligned} 41^{41} &\equiv (3^{18})^2 \times 3^5 \\ &\equiv 3^5 \equiv 27 \times 9 \equiv 8 \times 9 \equiv 72 \equiv 15 \pmod{19}. \end{aligned}$$

Hence the remainder is 15.

Solution 4.1

(a) By Exercise 3.1(a), the multiplicative inverse of 13 in $\mathbb{Z}_{30}$ is 7, so $M_{13}^{-1} = M_7$. Thus we need to find

$$M_7(15) = 7 \times_{30} 15 = 15,$$

which gives 'O';

$$M_7(28) = 7 \times_{30} 28 = 16,$$

which gives 'P';

$$M_7(5) = 7 \times_{30} 5 = 5,$$

which gives 'E';

$$M_7(2) = 7 \times_{30} 2 = 14,$$

which gives 'N'.

Thus the message was 'OPEN'.

(b) By Exercise 3.1(b), the multiplicative inverse of 25 in $\mathbb{Z}_{36}$ is 13, so $E_{25}^{-1} = E_{13}$. Thus we need to find

$$E_{13}(25),\ E_{13}(13),\ E_{13}(19).$$

Repeated squaring gives

25^{2^n}	25^1	25^2	25^4	25^8
$25^{2^n} \pmod{37}$	25	33	16	34

and so

$$\begin{aligned} E_{13}(25) &\equiv 25^{13} \\ &\equiv 25^1 \times 25^4 \times 25^8 \\ &\equiv 25 \times 16 \times 34 \\ &\equiv 30 \times 34 \equiv 21 \pmod{37}, \end{aligned}$$

which gives 'U'.

Repeated squaring gives

13^{2^n}	13^1	13^2	13^4	13^8
$13^{2^n} \pmod{37}$	13	21	34	9

and so

$$\begin{aligned} E_{13} &\equiv 13^{13} \\ &\equiv 13^1 \times 13^4 \times 13^8 \\ &\equiv 13 \times 34 \times 9 \\ &\equiv 35 \times 9 \equiv 19 \pmod{37}, \end{aligned}$$

which gives 'S'.

Repeated squaring gives

19^{2^n}	19^1	19^2	19^4	19^8
$19^{2^n} \pmod{37}$	19	28	7	12

and so

$$\begin{aligned} E_{13}(19) &\equiv 19^{13} \\ &\equiv 19^1 \times 19^4 \times 19^8 \\ &\equiv 19 \times 7 \times 12 \equiv 22 \times 12 \equiv 5 \pmod{37}, \end{aligned}$$

which gives 'E'.

Thus the message was 'USE'.

(c) Note that $33 = 3 \times 11$, so with $p = 3$ and $q = 11$ we obtain $(p-1)(q-1) = 20$. Thus, to find the inverse function for the RSA cipher R_{13} on $\mathbb{Z}_{33}$, we need to determine the multiplicative inverse of 13 in $\mathbb{Z}_{20}$. By Exercise 3.1(c), we know this to be 17, so $R_{13}^{-1} = R_{17}$. Thus we need to find

$$R_{17}(26), R_{17}(30), R_{17}(4), R_{17}(12), R_{17}(9), R_{17}(24).$$

Repeated squaring gives

26^{2^n}	26^1	26^2	26^4	26^8	26^{16}
$26^{2^n} \pmod{33}$	26	16	25	31	4

and so

$$\begin{aligned} R_{17}(26) &\equiv 26^{17} \\ &\equiv 26^1 \times 26^{16} \equiv 26 \times 4 \equiv 5 \pmod{33}, \end{aligned}$$

which gives 'E'.

In the same way, we find that

$$R_{17}(30) = 24,\ R_{17}(4) = 16,\ R_{17}(12) = 12,$$
$$R_{17}(9) = 15,\ R_{17}(24) = 18,$$

and so the message was 'EXPLORE'.

Index

The Open University
ISBN 0 7492 6653 8